PCT/JP2004/019124
15.12.2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１２月１７日

出願番号
Application Number: 特願２００３－４１９７６５

[ST. 10/C]: [ＪＰ２００３－４１９７６５]

出願人
Applicant(s): 松下電器産業株式会社

２００５年　１月２７日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００５－３００３４３２

【書類名】　特許願
【整理番号】　2022550300
【あて先】　特許庁長官殿
【国際特許分類】　G09L　1/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　野仲　真佐男
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　布田　裕一
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　大森　基司
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　山田　茂
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　井上　哲也
【発明者】
　【住所又は居所】　愛知県名古屋市中区栄２丁目６番１号白川ビル別館５Ｆ　株式会社松下電器情報システム名古屋研究所内
　【氏名】　熊崎　洋児
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100109210
　【弁理士】
　【氏名又は名称】　新居　広守
【手数料の表示】
　【予納台帳番号】　049515
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0213583

【書類名】特許請求の範囲
【請求項１】
コンテンツを配信するコンテンツ配信システムであって、
前記コンテンツ配信システムは、前記コンテンツを暗号化して配信するサーバと、暗号化された前記コンテンツを受信、復号化する複数の出力装置と、から構成され、前記サーバと前記出力装置のそれぞれは通信路を介して通信可能であって、さらに、各出力装置は、所定の鍵割当方法により個別に割り当てられた割当ノード復号化鍵群を保持しており、
前記鍵割当方法は、一以上の木構造を用いており、各々の前記木構造は複数のノードから構成され、前記複数のノードは複数の階層（第０階層から第ｎ階層：ｎは１以上の自然数）により分類され、ただし、前記第０階層は一つの前記ノードから構成され、前記木構造の全ての前記ノードに一以上のノード暗号化鍵及び対応するノード復号化鍵の組を設定し、前記第ｉ階層（ｉは１からｎまでの自然数）の前記ノードは、前記第０階層から前記第ｉ－１階層のいずれか一つの前記ノードである親ノードと線で結ばれており、前記第ｎ階層の前記ノード、および、前記第ｊ階層（ｊは１からｎ－１までの自然数）の前記ノードであり、前記第ｊ＋１階層から前記第ｎ階層のいずれの前記ノードにも線で結ばれていない前記ノードを末端ノードとし、前記末端ノードに対して、関連ノード集合は、前記末端ノードと、前記末端ノードの親ノードと、前記関連ノード集合に属するノードの親ノードから成り、前記関連ノード集合に属するノードに設定された前記ノード復号化鍵を割当ノード復号化鍵群とし、ノード暗号化鍵群を、全ての前記ノードに設定された前記ノード暗号化鍵とし、前記出力装置に前記末端ノードのいずれかを対応づけ、前記末端ノードの前記関連ノード集合に対応する前記割当ノード復号化鍵群を割り当てる方法であり、
前記サーバは、
前記鍵割当方法により予め与えられる前記ノード暗号化鍵群を保持する鍵情報格納部と、
前記ノード暗号化鍵群の中から一以上の前記ノード暗号化鍵を選定し選定ノード暗号化鍵群とし、前記選定ノード暗号化鍵群は、少なくとも前記末端ノードに設定されている前記ノード暗号化鍵を含み、かつ、前記末端ノード以外の前記ノードに設定されている前記ノード暗号化鍵を含み、前記選定ノード暗号化鍵群の中の前記ノード暗号化鍵の各々を用いて、予め与えられるコンテンツ復号化鍵を暗号化することによって、暗号化コンテンツ鍵群を生成するコンテンツ鍵選択部と、
外部から前記コンテンツを受信する入力部と、
前記コンテンツ復号化鍵に対応し予め与えられるコンテンツ暗号化鍵に基づき前記コンテンツを暗号化する暗号化部と、
前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群を前記出力装置に配信する送信部と、を備え、
前記出力装置は、
前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群を受信する第一受信部と、
前記鍵割当方法により予め与えられる前記割当ノード復号化鍵群を保持するノード鍵格納部と、
前記割当ノード復号化鍵群及び前記暗号化コンテンツ鍵群に基づき前記コンテンツ復号化鍵を取得する復号化鍵取得部と、
前記コンテンツ復号化鍵に基づき前記暗号化コンテンツを復号化する第一復号化部と、を備えることを特徴とする、コンテンツ配信システム。
【請求項２】
前記サーバは、さらに、複数の前記コンテンツを受信するとし、外部から前記コンテンツを受信した際に、前回前記コンテンツを暗号化する際に用いた一以上の前記コンテンツ暗号化鍵及び対応する前記コンテンツ復号化鍵の組とは異なる一以上の前記コンテンツ暗号化鍵及び対応する前記コンテンツ復号化鍵の組を新たに生成するコンテンツ鍵生成部を備えることを特徴とする、請求項１に記載のコンテンツ配信システム。
【請求項３】

前記サーバは、さらに、複数の前記コンテンツを受信するとし、前記コンテンツ鍵選択部は、さらに、前記サーバが外部から前記コンテンツを受信した際に、前回選定した前記末端ノードとは異なる前記末端ノードに設定されている前記ノード暗号化鍵を含む前記選定ノード暗号化鍵群を新たに作成することを特徴とする、請求項１または請求項２に記載のコンテンツ配信システム。

【請求項４】

前記サーバは、さらに、前記割当ノード復号化鍵群における前記ノード暗号化鍵の鍵選定情報を複数保持する鍵選定情報格納部を備え、

前記コンテンツ鍵選択部は、前記鍵選定情報格納部の保持している複数の前記鍵選定情報を基に、前記選定ノード暗号化鍵群を作成することを特徴とする、請求項１から請求項３のいずれか１項に記載のコンテンツ配信システム。

【請求項５】

前記サーバ及び前記出力装置は、さらに、前記選定ノード暗号化鍵群における前記ノード暗号化鍵の鍵選定情報と前記鍵選定情報を識別する鍵選定識別子を対応付けて複数保持している鍵選定情報格納部を備え、

前記コンテンツ鍵選択部は、前記鍵選定情報格納部の保持している複数の前記鍵選定情報のいずれかの前記鍵選定情報を基に前記選定ノード暗号化鍵群を作成し、基にした前記鍵選定情報に対応する前記鍵選定識別子を前記送信部へ出力し、

前記送信部は、前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群及び前記鍵選定識別子を前記出力装置に配信し、

前記第一受信部は、前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群及び前記鍵選定識別子を受信し、

前記復号化鍵取得部は、前記鍵選定情報格納部の保持している複数の前記鍵選定情報を用いて、前記割当ノード復号化鍵群及び前記暗号化コンテンツ鍵群及び前記鍵選定識別子を基に、前記コンテンツ復号化鍵を取得することを特徴とする、請求項１から請求項３のいずれか１項に記載のコンテンツ配信システム。

【請求項６】

前記コンテンツ鍵選択部は、前記鍵選定情報格納部が保持している複数の前記鍵選定情報の中からランダムに一つの前記鍵選定情報を選択し、選択された前記鍵選定情報を基に前記選定ノード暗号化鍵群を作成することを特徴とする、請求項４または請求項５に記載のコンテンツ配信システム。

【請求項７】

前記コンテンツ鍵選択部は、前記鍵選定情報格納部が保持している複数の前記鍵選定情報の中の前記鍵選定情報を周期的に一つ選択し、選択された前記鍵選定情報を基に選定ノード暗号化鍵群を作成することを特徴とする、請求項４または請求項５に記載のコンテンツ配信システム。

【請求項８】

前記鍵割当方法における木構造は、Ｎ分木（Ｎは２以上の自然数）であることを特徴とする、請求項１から請求項７のいずれか１項に記載のコンテンツ配信システム。

【請求項９】

前記コンテンツ配信システムは、さらに、前記通信路を介して前記出力装置のそれぞれとサーバに接続され、前記ノード暗号化鍵群及び複数の前記割当ノード復号化鍵群を配信する鍵発行センタを備え、

前記鍵発行センタは、

前記鍵割当方法に基づき、前記ノード暗号化鍵群及び複数の割当ノード復号化鍵群を生成するノード鍵生成部と、

前記ノード暗号化鍵群を前記サーバに送信する第一送信部と、

複数の前記割当ノード復号化鍵群と複数の前記出力装置の対応情報を保持する出力装置対応情報格納部と、

前記対応情報に基づき複数の前記割当ノード復号化鍵群を前記それぞれの出力装置に配

信する第二送信部と、を備え
　前記サーバは、
　受信した前記ノード暗号化鍵群を前記鍵情報格納部に格納する受信部を備え、
　前記出力装置は、
　受信した前記割当ノード復号化鍵群を前記ノード鍵格納部へ格納する第二受信部を備えることを特徴とする、請求項１から請求項８のいずれか１項に記載のコンテンツ配信システム。
【請求項１０】
　前記コンテンツ配信システムは、さらに、前記通信路を介して前記出力装置のそれぞれとサーバに接続され、前記ノード暗号化鍵群及び鍵更新情報を配信する鍵発行センタを備え、
　前記鍵発行センタは、
　予め各々の前記出力装置に与えられる個別鍵を保持する出力装置対応情報格納部と、
各々の前記出力装置に与えられる前記個別鍵を基に各々の前記出力装置に割り当てられた前記割当ノード復号化鍵群を暗号化し、鍵更新情報を生成する第一暗号化部と、
　前記鍵更新情報を前記出力装置へ配信する第二送信部とを備え、
　前記出力装置は、前記鍵更新情報を受信する第二受信部と、
予め与えられる前記個別鍵を保持する個別鍵格納部と、
　前記個別鍵に基づき受信した前記鍵更新情報の復号化を行い、復号化された前記割当ノード復号化鍵群を前記ノード鍵格納部へ格納する第二復号化部と、を備えることを特徴とする、請求項１から請求項８のいずれか１項に記載のコンテンツ配信システム。
【請求項１１】
　前記出力装置対応情報格納部は、さらに、各々の前記出力装置に対応付けられている出力装置識別子と前記割当ノード復号化鍵群の対応情報を保持し、
　前記鍵発行センタは、外部から前記出力装置識別子を受信した場合に、前記出力装置識別子を基に、前記出力装置対応情報格納部の保持している前記対応情報を更新し、さらに、前記ノード鍵生成要求を前記ノード鍵生成部へ出力する対応情報更新部を備え、
　前記ノード鍵生成部は、前記ノード鍵生成要求を受信した場合に、前記鍵割当方法に基づき、前記ノード暗号化鍵群及び複数の割当ノード復号化鍵群を生成することを特徴とする、請求項１０に記載のコンテンツ配信システム。
【請求項１２】
　前記ノード鍵生成部は、前記鍵割当方法に基づき、前記ノード暗号化鍵群及び複数の割当ノード復号化鍵群を生成した場合、前記第一暗号化部へ鍵更新情報生成要求を出力し、
　前記第一暗号化部は、前記鍵更新情報生成要求を受信した場合、各々の前記出力装置に与えられる前記個別鍵を基に各々の前記出力装置に割り当てられた前記割当ノード復号化鍵群を暗号化し、鍵更新情報を生成することを特徴とする、請求項１０または請求項１１に記載のコンテンツ配信システム。
【請求項１３】
　コンテンツを暗号化して配信するサーバと、通信路を介して前記サーバに接続され、前記コンテンツを受信する出力装置と、を備えるコンテンツ配信システムにおける出力装置であって、
　各出力装置は、さらに、所定の鍵割当方法により個別に割り当てられた割当ノード復号化鍵群を保持しており、
　前記サーバ及び前記出力装置は、さらに、前記割当ノード復号化鍵群における前記ノード暗号化鍵の鍵選定情報と前記鍵選定情報を識別する鍵選定識別子を対応付けて複数保持している鍵選定情報格納部を備え、
　前記鍵割当方法は、一以上の木構造を用いており、各々の前記木構造は複数のノードから構成され、前記複数のノードは複数の階層（第０階層から第ｎ階層：ｎは１以上の自然数）により分類され、ただし、前記第０階層は一つの前記ノードから構成され、前記木構造の全ての前記ノードに一以上のノード暗号化鍵及び対応するノード復号化鍵の組を設定

し、前記第ｉ階層（ｉは１からｎまでの自然数）の前記ノードは、前記第０階層から前記第ｉ－１階層のいずれか一つの前記ノードである親ノードと線で結ばれており、前記第ｎ階層の前記ノード、および、前記第ｊ階層（ｊは１からｎ－１までの自然数）の前記ノードであり、前記第ｊ＋１階層から前記第ｎ階層のいずれの前記ノードにも線で結ばれていない前記ノードを末端ノードとし、前記末端ノードに対して、関連ノード集合は、前記末端ノードと、前記末端ノードの親ノードと、前記関連ノード集合に属するノードの親ノードから成り、前記関連ノード集合に属するノードに設定された前記ノード復号化鍵を割当ノード復号化鍵群とし、ノード暗号化鍵群を、全ての前記ノードに設定された前記ノード暗号化鍵とし、前記出力装置に前記末端ノードのいずれかを対応づけ、前記末端ノードの前記関連ノード集合に対応する前記割当ノード復号化鍵群を割り当てる方法であり、

前記出力装置は、

外部から前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群及び前記鍵選定識別子を受信する第一受信部と、

前記鍵割当方法により予め与えられる前記割当ノード復号化鍵群を保持するノード鍵格納部と、

前記鍵選定情報格納部の保持している複数の前記鍵選定情報を用いて、前記割当ノード復号化鍵群及び前記暗号化コンテンツ鍵群及び前記鍵選定情報識別子を基に、前記コンテンツ復号化鍵を取得する復号化鍵取得部と、

前記コンテンツ復号化鍵に基づき前記暗号化コンテンツを復号化する第一復号化部と、を備えることを特徴とする、出力装置。

【請求項１４】

前記鍵割当方法における木構造は、Ｎ分木（Ｎは２以上の自然数）であることを特徴とする、請求項１３に記載の出力装置。

【請求項１５】

前記コンテンツ配信システムは、さらに、前記通信路を介して前記出力装置のそれぞれとサーバに接続され、前記ノード暗号化鍵群及び複数の前記割当ノード復号化鍵群を配信する鍵発行センタを備え、

さらに、外部から受信した前記割当ノード復号化鍵群を前記ノード鍵格納部へ格納する第二受信部と、を備えることを特徴とする、請求項１３または請求項１４に記載の出力装置。

【請求項１６】

前記コンテンツ配信システムは、さらに、前記通信路を介して前記出力装置のそれぞれとサーバに接続され、前記ノード暗号化鍵群及び鍵更新情報を配信する鍵発行センタを備え、

さらに、外部から前記鍵更新情報を受信する第二受信部と、

予め与えられる個別鍵を保持する個別鍵格納部と、

前記個別鍵に基づき受信した前記鍵更新情報の復号化を行い、復号化された前記割当ノード復号化鍵群を前記ノード鍵格納部へ格納する第二復号化部と、を備えることを特徴とする、請求項１３または請求項１４に記載のコンテンツ配信システム。

【請求項１７】

コンテンツを暗号化して配信するサーバと、通信路を介して前記サーバに接続され、前記コンテンツを受信する処理をコンピュータに実行させるプログラムであって、所定の鍵割当方法により個別に割り当てられた割当ノード復号化鍵群を保持しており、さらに、前記割当ノード復号化鍵群における複数の前記ノード暗号化鍵の鍵選定情報と前記鍵選定情報を識別する鍵選定識別子の対応情報を保持しており、

前記鍵割当方法は、一以上の木構造を用いており、各々の前記木構造は複数のノードから構成され、前記複数のノードは複数の階層（第０階層から第ｎ階層：ｎは１以上の自然数）により分類され、ただし、前記第０階層は一つの前記ノードから構成され、前記木構造の全ての前記ノードに一以上のノード暗号化鍵及び対応するノード復号化鍵の組を設定し、前記第ｉ階層（ｉは１からｎまでの自然数）の前記ノードは、前記第０階層から前記

第ｉ－１階層のいずれか一つの前記ノードである親ノードと線で結ばれており、前記第ｎ階層の前記ノード、および、前記第ｊ階層（ｊは１からｎ－１までの自然数）の前記ノードであり、前記第ｊ＋１階層から前記第ｎ階層のいずれの前記ノードにも線で結ばれていない前記ノードを末端ノードとし、前記末端ノードに対して、関連ノード集合は、前記末端ノードと、前記末端ノードの親ノードと、前記関連ノード集合に属するノードの親ノードから成り、前記関連ノード集合に属するノードに設定された前記ノード復号化鍵を割当ノード復号化鍵群とし、ノード暗号化鍵群を、全ての前記ノードに設定された前記ノード暗号化鍵とし、前記出力装置に前記末端ノードのいずれかを対応づけ、前記末端ノードの前記関連ノード集合に対応する前記割当ノード復号化鍵群を割り当てる方法であり、

外部から前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群及び前記鍵選定識別子を受信するステップと、

複数の前記鍵選定情報を用いて、前記割当ノード復号化鍵群及び前記暗号化コンテンツ鍵群及び前記鍵選定情報識別子を基に、前記コンテンツ復号化鍵を取得するステップと、

前記コンテンツ復号化鍵に基づき前記暗号化コンテンツを復号化するステップと、をコンピュータに実行させることを特徴とする、プログラム。

【請求項１８】

請求項１７に記載のプログラムを記録した媒体。

【請求項１９】

。さらに、前記鍵割当方法における木構造は、Ｎ分木（Ｎは２以上の自然数）であることを特徴とする、請求項１７に記載のプログラム。

【請求項２０】

請求項１９に記載のプログラムを記録した媒体。

【請求項２１】

さらに、前記通信路を介して前記プログラムと前記サーバに接続され、前記ノード暗号化鍵群及び複数の前記割当ノード復号化鍵群を配信する鍵発行センタを備え、

さらに、外部から前記割当ノード復号化鍵群を受信するステップと、をコンピュータに実行させることを特徴とする、請求項１７または請求項１９に記載のプログラム。

【請求項２２】

請求項２１に記載のプログラムを記録した媒体。

【請求項２３】

さらに、前記通信路を介して前記プログラムと前記サーバに接続され、前記ノード暗号化鍵群及び鍵更新情報を配信する鍵発行センタを備え、

さらに、外部から前記鍵更新情報を受信するステップと、予め与えられる個別鍵に基づき受信した前記鍵更新情報の復号化を行うステップと、をコンピュータに実行させることを特徴とする、請求項１７または請求項１９に記載のプログラム。

【請求項２４】

請求項２３に記載のプログラムを記録した媒体。

【請求項２５】

コンテンツを配信するコンテンツ配信方法であって、

前記コンテンツ配信方法は、所定の鍵割当方法を基に予め与えられたノード暗号化鍵群を用いて前記コンテンツを暗号化して配信するコンテンツ配信ステップと、前記鍵割当方法を基に予め与えられた割当ノード復号化鍵群を用いて暗号化された前記コンテンツを復号化するコンテンツ受信ステップと、から構成され、

前記鍵割当方法は、一以上の木構造を用いており、各々の前記木構造は複数のノードから構成され、前記複数のノードは複数の階層（第０階層から第ｎ階層：ｎは１以上の自然数）により分類され、ただし、前記第０階層は一つの前記ノードから構成され、前記木構造の全ての前記ノードに一以上のノード暗号化鍵及び対応するノード復号化鍵の組を設定し、前記第ｉ階層（ｉは１からｎまでの自然数）の前記ノードは、前記第０階層から前記第ｉ－１階層のいずれか一つの前記ノードである親ノードと線で結ばれており、前記第ｎ階層の前記ノード、および、前記第ｊ階層（ｊは１からｎ－１までの自然数）の前記ノー

ドであり、前記第ｊ＋１階層から前記第ｎ階層のいずれの前記ノードにも線で結ばれていない前記ノードを末端ノードとし、前記末端ノードに対して、関連ノード集合は、前記末端ノードと、前記末端ノードの親ノードと、前記関連ノード集合に属するノードの親ノードから成り、前記関連ノード集合に属するノードに設定された前記ノード復号化鍵を割当ノード復号化鍵群とし、ノード暗号化鍵群を、全ての前記ノードに設定された前記ノード暗号化鍵とし、前記コンテンツ受信ステップに前記末端ノードのいずれかを対応づけ、前記末端ノードの前記関連ノード集合に対応する前記割当ノード復号化鍵群を割り当てる方法であり、

前記コンテンツ配信ステップは、

前記鍵割当方法により予め与えられる前記ノード暗号化鍵群の中から一以上の前記ノード暗号化鍵を選定し選定ノード暗号化鍵群とし、前記選定ノード暗号化鍵群は、少なくとも前記末端ノードに設定されている前記ノード暗号化鍵を含み、かつ、前記末端ノード以外の前記ノードに設定されている前記ノード暗号化鍵を含み、前記選定ノード暗号化鍵群の中の前記ノード暗号化鍵の各々を用いて、予め与えられるコンテンツ復号化鍵を暗号化することによって、暗号化コンテンツ鍵群を生成するステップと、

外部から前記コンテンツを受信するステップと、

前記コンテンツ復号化鍵に対応し予め与えられるコンテンツ暗号化鍵に基づき前記コンテンツを暗号化するステップと、

前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群を前記出力装置に配信するステップと、を含み、

前記コンテンツ受信ステップは、前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群を受信するステップと、前記鍵割当方法により予め与えられる前記割当ノード復号化鍵群及び前記暗号化コンテンツ鍵群に基づき前記コンテンツ復号化鍵を取得するステップと、前記コンテンツ復号化鍵に基づき前記暗号化コンテンツを復号化するステップと、を含むことを特徴とする、コンテンツ配信方法。

【書類名】明細書
【発明の名称】コンテンツ配信システム
【技術分野】
【０００１】
本発明は、映画や音楽などのデジタルコンテンツを複数の出力装置に暗号化して配信するコンテンツ配信システムに関し、特に、暗号化されたコンテンツを出力装置で復号化する際に用いる鍵を出力装置毎に個別にすることで、もし出力装置に割り当てられている鍵が漏洩しても、その漏洩元の出力装置を追跡可能な技術に関する。
【背景技術】
【０００２】
ＡＤＳＬや光ファイバーなどに代表される高速通信路の普及に伴い、デジタル化された音楽や映像等のコンテンツを通信路を介して提供するサービスが盛んに行われるようになった。このようなサービスの普及に伴い、不正コピーなどに代表されるコンテンツ不正利用を防止する著作権保護方式が必要となってきている。一般に、このコンテンツ不正利用を防止する著作権保護方式には、暗号技術が用いられる。つまり、あるコンテンツ暗号化鍵を用いてデジタルコンテンツを暗号化して通信路を介して配布し、そのコンテンツ暗号化鍵に対応するコンテンツ復号化鍵を与えられている出力装置のみが、暗号化されたコンテンツを復号化して、元のデジタルコンテンツの再生を行うことが出来るというものである。
【０００３】
ところで、通常、出力装置に与えられているコンテンツ復号化鍵は秘密に保持されるが、端末の不正解析などによって、攻撃者が全装置共通に与えられているコンテンツ復号化鍵を取得する可能性がある。ある端末に与えられているコンテンツ復号化鍵が一旦漏洩してしまうと、攻撃者はこの漏洩元の追跡が不可能なコンテンツ復号化鍵を用いてデジタルコンテンツの復号化を行う端末を作成し、コンテンツの不正利用を行うおそれがある。そのようなコンテンツ不正利用を防ぐ手段の一つとして、出力装置毎に個別の鍵を持たせることによって、漏洩元の出力装置の追跡を可能にするシステムが考えられる。全出力装置に同じデータを送るような放送局型のコンテンツ配信において、コンテンツ不正利用を防止する方式としては、例えば下記非特許文献１に記載されたコンテンツ配信システムがある。
【０００４】
図３４は、前記非特許文献１に記載された従来のコンテンツ配信システムを示すものである。図３４において、通信路９０は、後述する鍵発行センタ９１及びサーバ９２及び複数の出力装置９３ａ～９３ｎを接続している通信路であり、インターネット等のネットワークで実現されている。鍵発行センタ９１は、コンテンツＣＮＴの暗号化及び復号化を行うコンテンツ暗号化鍵ＣＥＫ、コンテンツ復号化鍵ＣＤＫをそれぞれ作成し、コンテンツ暗号化鍵ＣＥＫをサーバ９２に、コンテンツ復号化鍵ＣＤＫを鍵更新情報ＵＰＤＫＥＹ＝Ｅｎｃ（ＩＫａ，ＣＤＫ）||Ｅｎｃ（ＩＫｂ，ＣＤＫ）||・・・Ｅｎｃ（ＩＫｎ，ＣＤＫ）として複数の出力装置９３ａ～９３ｎに配信する。ここで、Ｅｎｃ（Ｋ，Ｐ）は暗号化鍵Ｋを用いて平文Ｐを暗号化した際の暗号文を意味する。また、ＩＫａ・・・ＩＫｎは、鍵発行センタ９１と複数の出力装置９３ａ～９３ｎの全ての組に予め一つ与えられる個別鍵のことであり、例えば鍵発行センタ９１と出力装置９３ａは個別鍵ＩＫａを、鍵発行センタ９１と出力装置９３ｂは個別鍵ＩＫｂを、鍵発行センタ９１と出力装置９３ｎは個別鍵ＩＫｎを予め共有しているとする。サーバ９２はコンテンツ暗号化鍵ＣＥＫを基にコンテンツＣＮＴの暗号化を行い、暗号化されたコンテンツＥＮＣＣＮＴを複数の出力装置９３ａ～９３ｎに配信し、複数の出力装置９３ａ～９３ｎは鍵更新情報ＵＰＤＫＥＹを基に受信した暗号化コンテンツＥＮＣＣＮＴの復号化を行い、その復号化コンテンツＤＥＣＣＮＴを外部へ出力する。ここで、コンテンツ暗号化鍵ＣＥＫ及びコンテンツ復号化鍵ＣＤＫは、全ての出力装置９３ａ～９３ｎにおいて共通の値である。そのため、ある個別鍵を取得した攻撃者が、漏洩元の追跡が不可能なコンテンツ復号化鍵ＣＤＫを埋め込んだ

不正な出力装置を作成する場合が考えられる。しかし、このようなコンテンツ復号化鍵ＣＤＫを埋め込んだ不正な出力装置は、鍵発行センタ９１がコンテンツ暗号化鍵ＣＥＫ及びコンテンツ復号化鍵ＣＤＫを新たな値に更新することで以後コンテンツを利用出来ないように無効化することができる。

【０００５】

ここでは、各構成要素の動作についてもう少し詳細に説明する。まず、全ての出力装置９３ａ～９３ｎでコンテンツ復号化鍵ＣＤＫを共有する方法について説明する。初めに、鍵発行センタ９１は、コンテンツ暗号化鍵ＣＥＫ及びコンテンツ復号化鍵ＣＤＫを生成し、そのコンテンツ暗号化鍵ＣＥＫをサーバ９２へ送信する。そして、それぞれの出力装置９３ａ～９３ｎと予め共有している個別鍵ＩＫａ、ＩＫｂ，・・・ＩＫｎに基づき、そのコンテンツ復号化鍵ＣＤＫを暗号化し、その各暗号文Ｅｎｃ（ＩＫａ，ＣＤＫ）、Ｅｎｃ（ＩＫｂ，ＣＤＫ）、・・・、Ｅｎｃ（ＩＫｎ，ＣＤＫ）を結合した値を鍵更新情報ＵＰＤＫＥＹ＝Ｅｎｃ（ＩＫａ，ＣＤＫ）||Ｅｎｃ（ＩＫｂ，ＣＤＫ）||・・・Ｅｎｃ（ＩＫｎ，ＣＤＫ）として複数の出力装置９３ａ～９３ｎへ向けて配信する。サーバ９２はコンテンツ暗号化鍵ＣＥＫを受信し、また、出力装置９３ａは、鍵更新情報ＵＰＤＫＥＹを受信し、鍵更新情報ＵＰＤＫＥＹの中から自身の持つ個別鍵ＩＫａに対応する暗号文Ｅｎｃ（ＩＫａ，ＣＤＫ）を抜き出し、個別鍵ＩＫａに基づき暗号文Ｅｎｃ（ＩＫａ，ＣＤＫ）の復号化を行い、コンテンツ復号化鍵ＣＤＫを取得する。なお、出力装置９３ａ以外の出力装置９３ｂ～９３ｎの場合も、出力装置９３ａと同様に、各々の出力装置が持つ個別鍵に対応する暗号文を鍵更新情報ＵＰＤＫＥＹから抜き出し、その暗号文を復号化することで、コンテンツ復号化鍵ＣＤＫを取得する。こうすることによって、全出力装置９３ａ～９３ｎでコンテンツ復号化鍵ＣＤＫを共有することが出来る。

【０００６】

次に、コンテンツを配信する場合の動作について説明する。まず、サーバ９２は、外部からコンテンツＣＮＴを受け取り、コンテンツ暗号化鍵ＣＥＫに基づきそのコンテンツＣＮＴの暗号化を行い、その暗号化コンテンツＥＮＣＣＮＴ＝Ｅｎｃ（ＣＥＫ，ＣＮＴ）を複数の出力装置９３ａ～９３ｎへ向けて配信する。暗号化コンテンツＥＮＣＣＮＴを受信した複数の出力装置９３ａ～９３ｎは、コンテンツ復号化鍵ＣＤＫに基づき暗号化コンテンツＥＮＣＣＮＴの復号化を行い、その復号化コンテンツＤＥＣＣＮＴを外部へ出力する。

【０００７】

なお、鍵発行センタ９１はある特定の個別鍵を有する出力装置を無効化し、コンテンツＣＮＴを復号化出来ないようにすることも出来る。ここでは、出力装置９３ａの個別鍵を有する出力機器を無効化する場合について説明する。まず、鍵発行センタ９１は外部から、出力装置９３ａを識別する出力装置識別子ＡＩＤａを受け取り、コンテンツ暗号化鍵ＣＥＫ及びコンテンツ復号化鍵ＣＤＫを新たに生成し、そのコンテンツ暗号化鍵ＣＥＫをサーバ９２に送信する。その後、出力装置識別子ＡＩＤａに対応する出力装置９３ａと予め共有している個別鍵ＩＫａを除く全ての個別鍵ＩＫｂ～ＩＫｎを用いて、そのコンテンツ復号化鍵ＣＤＫの暗号化を行い、その各暗号文Ｅｎｃ（ＩＫｂ，ＣＤＫ）、・・・、Ｅｎｃ（ＩＫｎ，ＣＤＫ）を結合した値を鍵更新情報ＵＰＤＫＥＹ＝Ｅｎｃ（ＩＫｂ，ＣＤＫ）||・・・Ｅｎｃ（ＩＫｎ，ＣＤＫ）として複数の出力装置９３ａ～９３ｎへ配信する。そうすることにより、出力装置識別子ＡＩＤａに対応する出力装置９３ａ以外の出力装置９３ｂ～９３ｎではコンテンツ復号化鍵ＣＤＫを取得することが出来るため、暗号化コンテンツＥＮＣＣＮＴ＝Ｅｎｃ（ＣＤＫ，ＣＮＴ）を正しく復号化出来るが、出力装置識別子ＡＩＤａに対応する出力装置９３ａではコンテンツ復号化鍵ＣＤＫを取得出来ないので、暗号化コンテンツＥＮＣＣＮＴ＝Ｅｎｃ（ＣＤＫ，ＣＮＴ）を復号化出来なくすることが出来る。なお、出力装置９３ａ以外の出力装置９３ｂ～９３ｎを無効化する場合も、出力装置９３ａの場合と同様の動作となるが、コンテンツ復号化鍵ＣＤＫを暗号化するのに用いる個別鍵が変わる点が異なる。このようにすることによって、鍵発行センタ９１は、出力装置を無効化することも出来る。

【０００８】
このようなシステムにより、もし攻撃者によって、出力装置９３ａ～９３ｎのうちの何れかの出力装置に埋め込まれている個別鍵が不正に取得され、攻撃者がその個別鍵を用いた出力装置を作ったとしても、その出力装置に埋め込まれている個別鍵から漏洩元の出力装置を追跡することが出来るため、対象出力装置の無効化などの対策を打つことが可能となる。

【非特許文献１】「デジタル放送局システムのしくみ」、映像情報メディア学会　編、オーム出版局

【発明の開示】
【発明が解決しようとする課題】
【０００９】
しかしながら、先に述べた従来の構成では、コンテンツ復号化鍵を埋め込んだ不正な出力装置を無効化するために、鍵発行センタがコンテンツ暗号化鍵及び対応するコンテンツ復号化鍵を更新したときに、出力装置へ配信する鍵更新情報のデータサイズが出力装置の数に比例して大きくなるという課題を有していた。

本発明は、上記課題を解決するもので、コンテンツ復号化鍵を埋め込んだ不正な出力装置を無効化するために、鍵発行センタがコンテンツ暗号化鍵及び対応するコンテンツ復号化鍵を更新したときに、出力装置へ配信するデータサイズを削減することが可能なコンテンツ配信システムを提供することを目的とする。

【課題を解決するための手段】
【００１０】
請求項１における発明は、コンテンツを配信するコンテンツ配信システムであって、前記コンテンツ配信システムは、前記コンテンツを暗号化して配信するサーバと、暗号化された前記コンテンツを受信、復号化する複数の出力装置と、から構成され、前記サーバと前記出力装置のそれぞれは通信路を介して通信可能であって、さらに、各出力装置は、所定の鍵割当方法により個別に割り当てられた割当ノード復号化鍵群を保持しており、前記鍵割当方法は、一以上の木構造を用いており、各々の前記木構造は複数のノードから構成され、前記複数のノードは複数の階層（第０階層から第ｎ階層：ｎは１以上の自然数）により分類され、ただし、前記第０階層は一つの前記ノードから構成され、前記木構造の全ての前記ノードに一以上のノード暗号化鍵及び対応するノード復号化鍵の組を設定し、前記第ｉ階層（ｉは１からｎまでの自然数）の前記ノードは、前記第０階層から前記第ｉ－１階層のいずれか一つの前記ノードである親ノードと線で結ばれており、前記第ｎ階層の前記ノード、および、前記第ｊ階層（ｊは１からｎ－１までの自然数）の前記ノードであり、前記第ｊ＋１階層から前記第ｎ階層のいずれの前記ノードにも線で結ばれていない前記ノードを末端ノードとし、前記末端ノードに対して、関連ノード集合は、前記末端ノードと、前記末端ノードの親ノードと、前記関連ノード集合に属するノードの親ノードから成り、前記関連ノード集合に属するノードに設定された前記ノード復号化鍵を割当ノード復号化鍵群とし、ノード暗号化鍵群を、全ての前記ノードに設定された前記ノード暗号化鍵とし、前記出力装置に前記末端ノードのいずれかを対応づけ、前記末端ノードの前記関連ノード集合に対応する前記割当ノード復号化鍵群を割り当てる方法であり、前記サーバは、前記鍵割当方法により予め与えられる前記ノード暗号化鍵群を保持する鍵情報格納部と、前記ノード暗号化鍵群の中から一以上の前記ノード暗号化鍵を選定し選定ノード暗号化鍵群とし、前記選定ノード暗号化鍵群は、少なくとも前記末端ノードに設定されている前記ノード暗号化鍵を含み、かつ、前記末端ノード以外の前記ノードに設定されている前記ノード暗号化鍵を含み、前記選定ノード暗号化鍵群の中の前記ノード暗号化鍵の各々を用いて、予め与えられるコンテンツ復号化鍵を暗号化することによって、暗号化コンテンツ鍵群を生成するコンテンツ鍵選択部と、外部から前記コンテンツを受信する入力部と、前記コンテンツ復号化鍵に対応し予め与えられるコンテンツ暗号化鍵に基づき前記コンテンツを暗号化する暗号化部と、前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群を前記出力装置に配信する送信部と、を備え、前記出力装置は、前記暗号化コンテンツ及び前

記暗号化コンテンツ鍵群を受信する第一受信部と、前記鍵割当方法により予め与えられる前記割当ノード復号化鍵群を保持するノード鍵格納部と、前記割当ノード復号化鍵群及び前記暗号化コンテンツ鍵群に基づき前記コンテンツ復号化鍵を取得する復号化鍵取得部と、前記コンテンツ復号化鍵に基づき前記暗号化コンテンツを復号化する第一復号化部と、を備えることを特徴とする。

【００１１】

請求項２における発明は、請求項１に記載のコンテンツ配信システムであって、前記サーバは、さらに、複数の前記コンテンツを受信するとし、外部から前記コンテンツを受信した際に、前回前記コンテンツを暗号化する際に用いた一以上の前記コンテンツ暗号化鍵及び対応する前記コンテンツ復号化鍵の組とは異なる一以上の前記コンテンツ暗号化鍵及び対応する前記コンテンツ復号化鍵の組を新たに生成するコンテンツ鍵生成部を備えることを特徴とする。

【００１２】

請求項３における発明は、請求項１または請求項２に記載のコンテンツ配信システムであって、前記サーバは、さらに、複数の前記コンテンツを受信するとし、前記コンテンツ鍵選択部は、さらに、前記サーバが外部から前記コンテンツを受信した際に、前回選定した前記末端ノードとは異なる前記末端ノードに設定されている前記ノード暗号化鍵を含む前記選定ノード暗号化鍵群を新たに作成することを特徴とする。

【００１３】

請求項４における発明は、請求項１から請求項３のいずれか１項に記載のコンテンツ配信システムであって、前記サーバは、さらに、前記割当ノード復号化鍵群における前記ノード暗号化鍵の鍵選定情報を複数保持する鍵選定情報格納部を備え、前記コンテンツ鍵選択部は、前記鍵選定情報格納部の保持している複数の前記鍵選定情報を基に、前記選定ノード暗号化鍵群を作成することを特徴とする。

【００１４】

請求項５における発明は、請求項１から請求項３のいずれか１項に記載のコンテンツ配信システムであって、前記サーバ及び前記出力装置は、さらに、前記選定ノード暗号化鍵群における前記ノード暗号化鍵の鍵選定情報と前記鍵選定情報を識別する鍵選定識別子を対応付けて複数保持している鍵選定情報格納部を備え、前記コンテンツ鍵選択部は、前記鍵選定情報格納部の保持している複数の前記鍵選定情報のいずれかの前記鍵選定情報を基に前記選定ノード暗号化鍵群を作成し、基にした前記鍵選定情報に対応する前記鍵選定識別子を前記送信部へ出力し、前記送信部は、前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群及び前記鍵選定識別子を前記出力装置に配信し、前記第一受信部は、前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群及び前記鍵選定識別子を受信し、前記復号化鍵取得部は、前記鍵選定情報格納部の保持している複数の前記鍵選定情報を用いて、前記割当ノード復号化鍵群及び前記暗号化コンテンツ鍵群及び前記鍵選定識別子を基に、前記コンテンツ復号化鍵を取得することを特徴とする。

【００１５】

請求項６における発明は、請求項４または請求項５に記載のコンテンツ配信システムであって、前記コンテンツ鍵選択部は、前記鍵選定情報格納部が保持している複数の前記鍵選定情報の中からランダムに一つの前記鍵選定情報を選択し、選択された前記鍵選定情報を基に前記選定ノード暗号化鍵群を作成することを特徴とする。

請求項７における発明は、請求項４または請求項５に記載のコンテンツ配信システムであって、前記コンテンツ鍵選択部は、前記鍵選定情報格納部が保持している複数の前記鍵選定情報の中の前記鍵選定情報を周期的に一つ選択し、選択された前記鍵選定情報を基に選定ノード暗号化鍵群を作成することを特徴とする。

【００１６】

請求項８における発明は、請求項１から請求項７のいずれか１項に記載のコンテンツ配信システムであって、前記鍵割当方法における木構造は、Ｎ分木（Ｎは２以上の自然数）であることを特徴とする。

請求項９における発明は、請求項１から請求項８のいずれか１項に記載のコンテンツ配信システムであって、前記コンテンツ配信システムは、さらに、前記通信路を介して前記出力装置のそれぞれとサーバに接続され、前記ノード暗号化鍵群及び複数の前記割当ノード復号化鍵群を配信する鍵発行センタを備え、前記鍵発行センタは、前記鍵割当方法に基づき、前記ノード暗号化鍵群及び複数の割当ノード復号化鍵群を生成するノード鍵生成部と、前記ノード暗号化鍵群を前記サーバに送信する第一送信部と、複数の前記割当ノード復号化鍵群と複数の前記出力装置の対応情報を保持する出力装置対応情報格納部と、前記対応情報に基づき複数の前記割当ノード復号化鍵群を前記それぞれの出力装置に配信する第二送信部と、を備え、前記サーバは、受信した前記ノード暗号化鍵群を前記鍵情報格納部に格納する受信部を備え、前記出力装置は、受信した前記割当ノード復号化鍵群を前記ノード鍵格納部へ格納する第二受信部を備えることを特徴とする。

【００１７】

請求項１０における発明は、請求項１から請求項８のいずれか１項に記載のコンテンツ配信システムであって、前記コンテンツ配信システムは、さらに、前記通信路を介して前記出力装置のそれぞれとサーバに接続され、前記ノード暗号化鍵群及び鍵更新情報を配信する鍵発行センタを備え、前記鍵発行センタは、予め各々の前記出力装置に与えられる個別鍵を保持する出力装置対応情報格納部と、各々の前記出力装置に与えられる前記個別鍵を基に各々の前記出力装置に割り当てられた前記割当ノード復号化鍵群を暗号化し、鍵更新情報を生成する第一暗号化部と、前記鍵更新情報を前記出力装置へ配信する第二送信部とを備え、前記出力装置は、前記鍵更新情報を受信する第二受信部と、予め与えられる前記個別鍵を保持する個別鍵格納部と、前記個別鍵に基づき受信した前記鍵更新情報の復号化を行い、復号化された前記割当ノード復号化鍵群を前記ノード鍵格納部へ格納する第二復号化部と、を備えることを特徴とする。

【００１８】

請求項１１における発明は、請求項１０に記載のコンテンツ配信システムであって、前記出力装置対応情報格納部は、さらに、各々の前記出力装置に対応付けられている出力装置識別子と前記割当ノード復号化鍵群の対応情報を保持し、前記鍵発行センタは、外部から前記出力装置識別子を受信した場合に、前記出力装置識別子を基に、前記出力装置対応情報格納部の保持している前記対応情報を更新し、さらに、前記ノード鍵生成要求を前記ノード鍵生成部へ出力する対応情報更新部を備え、前記ノード鍵生成部は、前記ノード鍵生成要求を受信した場合に、前記鍵割当方法に基づき、前記ノード暗号化鍵群及び複数の割当ノード復号化鍵群を生成することを特徴とする。

【００１９】

請求項１２における発明は、請求項１０または請求項１１に記載のコンテンツ配信システムであって、前記ノード鍵生成部は、前記鍵割当方法に基づき、前記ノード暗号化鍵群及び複数の割当ノード復号化鍵群を生成した場合、前記第一暗号化部へ鍵更新情報生成要求を出力し、前記第一暗号化部は、前記鍵更新情報生成要求を受信した場合、各々の前記出力装置に与えられる前記個別鍵を基に各々の前記出力装置に割り当てられた前記割当ノード復号化鍵群を暗号化し、鍵更新情報を生成することを特徴とする。

【００２０】

請求項１３における発明は、コンテンツを暗号化して配信するサーバと、通信路を介して前記サーバに接続され、前記コンテンツを受信する出力装置と、を備えるコンテンツ配信システムにおける出力装置であって、さらに、各出力装置は、所定の鍵割当方法により個別に割り当てられた割当ノード復号化鍵群を保持しており、前記サーバ及び前記出力装置は、さらに、前記割当ノード復号化鍵群における前記ノード暗号化鍵の鍵選定情報と前記鍵選定情報を識別する鍵選定識別子を対応付けて複数保持している鍵選定情報格納部を備え、前記鍵割当方法は、一以上の木構造を用いており、各々の前記木構造は複数のノードから構成され、前記複数のノードは複数の階層（第０階層から第ｎ階層：ｎは１以上の自然数）により分類され、ただし、前記第０階層は一つの前記ノードから構成され、前記木構造の全ての前記ノードに一以上のノード暗号化鍵及び対応するノード復号化鍵の組を

設定し、前記第ｉ階層（ｉは１からｎまでの自然数）の前記ノードは、前記第０階層から前記第ｉ－１階層のいずれか一つの前記ノードである親ノードと線で結ばれており、前記第ｎ階層の前記ノード、および、前記第ｊ階層（ｊは１からｎ－１までの自然数）の前記ノードであり、前記第ｊ＋１階層から前記第ｎ階層のいずれの前記ノードにも線で結ばれていない前記ノードを末端ノードとし、前記末端ノードに対して、関連ノード集合は、前記末端ノードと、前記末端ノードの親ノードと、前記関連ノード集合に属するノードの親ノードから成り、前記関連ノード集合に属するノードに設定された前記ノード復号化鍵を割当ノード復号化鍵群とし、ノード暗号化鍵群を、全ての前記ノードに設定された前記ノード暗号化鍵とし、前記出力装置に前記末端ノードのいずれかを対応づけ、前記末端ノードの前記関連ノード集合に対応する前記割当ノード復号化鍵群を割り当てる方法であり、前記出力装置は、外部から前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群及び前記鍵選定識別子を受信する第一受信部と、前記鍵割当方法により予め与えられる前記割当ノード復号化鍵群を保持するノード鍵格納部と、前記鍵選定情報格納部の保持している複数の前記鍵選定情報を用いて、前記割当ノード復号化鍵群及び前記暗号化コンテンツ鍵群及び前記鍵選定情報識別子を基に、前記コンテンツ復号化鍵を取得する復号化鍵取得部と、前記コンテンツ復号化鍵に基づき前記暗号化コンテンツを復号化する第一復号化部と、を備えることを特徴とする。

【００２１】

請求項１４における発明は、請求項１３に記載の出力装置であって、前記鍵割当方法における木構造は、Ｎ分木（Ｎは２以上の自然数）であることを特徴とする。

請求項１５における発明は、請求項１３または請求項１４に記載の出力装置であって、前記コンテンツ配信システムは、さらに、前記通信路を介して前記出力装置のそれぞれとサーバに接続され、前記ノード暗号化鍵群及び複数の前記割当ノード復号化鍵群を配信する鍵発行センタを備え、さらに、外部から受信した前記割当ノード復号化鍵群を前記ノード鍵格納部へ格納する第二受信部と、を備えることを特徴とする。

【００２２】

請求項１６における発明は、請求項１３または請求項１４に記載のコンテンツ配信システムであって、前記コンテンツ配信システムは、さらに、前記通信路を介して前記出力装置のそれぞれとサーバに接続され、前記ノード暗号化鍵群及び鍵更新情報を配信する鍵発行センタを備え、さらに、外部から前記鍵更新情報を受信する第二受信部と、予め与えられる個別鍵を保持する個別鍵格納部と、前記個別鍵に基づき受信した前記鍵更新情報の復号化を行い、復号化された前記割当ノード復号化鍵群を前記ノード鍵格納部へ格納する第二復号化部と、を備えることを特徴とする。

【００２３】

請求項１７における発明は、コンテンツを暗号化して配信するサーバと、通信路を介して前記サーバに接続され、前記コンテンツを受信する処理をコンピュータに実行させるプログラムであって、所定の鍵割当方法により個別に割り当てられた割当ノード復号化鍵群を保持しており、さらに、前記割当ノード復号化鍵群における複数の前記ノード暗号化鍵の鍵選定情報と前記鍵選定情報を識別する鍵選定識別子の対応情報を保持しており、前記鍵割当方法は、一以上の木構造を用いており、各々の前記木構造は複数のノードから構成され、前記複数のノードは複数の階層（第０階層から第ｎ階層：ｎは１以上の自然数）により分類され、ただし、前記第０階層は一つの前記ノードから構成され、前記木構造の全ての前記ノードに一以上のノード暗号化鍵及び対応するノード復号化鍵の組を設定し、前記第ｉ階層（ｉは１からｎまでの自然数）の前記ノードは、前記第０階層から前記第ｉ－１階層のいずれか一つの前記ノードである親ノードと線で結ばれており、前記第ｎ階層の前記ノード、および、前記第ｊ階層（ｊは１からｎ－１までの自然数）の前記ノードであり、前記第ｊ＋１階層から前記第ｎ階層のいずれの前記ノードにも線で結ばれていない前記ノードを末端ノードとし、前記末端ノードに対して、関連ノード集合は、前記末端ノードと、前記末端ノードの親ノードと、前記関連ノード集合に属するノードの親ノードから成り、前記関連ノード集合に属するノードに設定された前記ノード復号化鍵を割当ノード

復号化鍵群とし、ノード暗号化鍵群を、全ての前記ノードに設定された前記ノード暗号化鍵とし、前記出力装置に前記末端ノードのいずれかを対応づけ、前記末端ノードの前記関連ノード集合に対応する前記割当ノード復号化鍵群を割り当てる方法であり、外部から前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群及び前記鍵選定識別子を受信するステップと、複数の前記鍵選定情報を用いて、前記割当ノード復号化鍵群及び前記暗号化コンテンツ鍵群及び前記鍵選定情報識別子を基に、前記コンテンツ復号化鍵を取得するステップと、前記コンテンツ復号化鍵に基づき前記暗号化コンテンツを復号化するステップと、をコンピュータに実行させることを特徴とする。

【００２４】

請求項１８における発明は、請求項１７に記載のプログラムを媒体に記録することを特長とする。

請求項１９における発明は、請求項１７に記載のプログラムであって、さらに、前記鍵割当方法における木構造は、Ｎ分木（Ｎは２以上の自然数）であることを特徴とする。

請求項２０における発明は、請求項１９に記載のプログラムを媒体に記録することを特徴とする。

【００２５】

請求項２１における発明は、請求項１７または請求項１９に記載のプログラムであって、さらに、前記通信路を介して前記プログラムと前記サーバに接続され、前記ノード暗号化鍵群及び複数の前記割当ノード復号化鍵群を配信する鍵発行センタを備え、さらに、外部から前記割当ノード復号化鍵群を受信するステップと、をコンピュータに実行させることを特徴とする。

【００２６】

請求項２２における発明は、請求項２１に記載のプログラムを媒体に記録することを特徴とする。

請求項２３における発明は、請求項１７または請求項１９に記載のプログラムであって、さらに、前記通信路を介して前記プログラムと前記サーバに接続され、前記ノード暗号化鍵群及び鍵更新情報を配信する鍵発行センタを備え、さらに、外部から前記鍵更新情報を受信するステップと、予め与えられる個別鍵に基づき受信した前記鍵更新情報の復号化を行うステップと、をコンピュータに実行させることを特徴とする。

【００２７】

請求項２４における発明は、請求項２３に記載のプログラムを記録した媒体。

請求項２５における発明は、コンテンツを配信するコンテンツ配信方法であって、前記コンテンツ配信方法は、所定の鍵割当方法を基に予め与えられたノード暗号化鍵群を用いて前記コンテンツを暗号化して配信するコンテンツ配信ステップと、前記鍵割当方法を基に予め与えられた割当ノード復号化鍵群を用いて暗号化された前記コンテンツを復号化するコンテンツ受信ステップと、から構成され、前記鍵割当方法は、一以上の木構造を用いており、各々の前記木構造は複数のノードから構成され、前記複数のノードは複数の階層（第０階層から第ｎ階層：ｎは１以上の自然数）により分類され、ただし、前記第０階層は一つの前記ノードから構成され、前記木構造の全ての前記ノードに一以上のノード暗号化鍵及び対応するノード復号化鍵の組を設定し、前記第ｉ階層（ｉは１からｎまでの自然数）の前記ノードは、前記第０階層から前記第ｉ－１階層のいずれか一つの前記ノードである親ノードと線で結ばれており、前記第ｎ階層の前記ノード、および、前記第ｊ階層（ｊは１からｎ－１までの自然数）の前記ノードであり、前記第ｊ＋１階層から前記第ｎ階層のいずれの前記ノードにも線で結ばれていない前記ノードを末端ノードとし、前記末端ノードに対して、関連ノード集合は、前記末端ノードと、前記末端ノードの親ノードと、前記関連ノード集合に属するノードの親ノードから成り、前記関連ノード集合に属するノードに設定された前記ノード復号化鍵を割当ノード復号化鍵群とし、ノード暗号化鍵群を、全ての前記ノードに設定された前記ノード暗号化鍵とし、前記コンテンツ受信ステップに前記末端ノードのいずれかを対応づけ、前記末端ノードの前記関連ノード集合に対応する前記割当ノード復号化鍵群を割り当てる方法であり、前記コンテンツ配信ステップは、

前記鍵割当方法により予め与えられる前記ノード暗号化鍵群の中から一以上の前記ノード暗号化鍵を選定し選定ノード暗号化鍵群とし、前記選定ノード暗号化鍵群は、少なくとも前記末端ノードに設定されている前記ノード暗号化鍵を含み、かつ、前記末端ノード以外の前記ノードに設定されている前記ノード暗号化鍵を含み、前記選定ノード暗号化鍵群の中の前記ノード暗号化鍵の各々を用いて、予め与えられるコンテンツ復号化鍵を暗号化することによって、暗号化コンテンツ鍵群を生成するステップと、外部から前記コンテンツを受信するステップと、前記コンテンツ復号化鍵に対応し予め与えられるコンテンツ暗号化鍵に基づき前記コンテンツを暗号化するステップと、前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群を前記出力装置に配信するステップと、を含み、前記コンテンツ受信ステップは、前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群を受信するステップと、前記鍵割当方法により予め与えられる前記割当ノード復号化鍵群及び前記暗号化コンテンツ鍵群に基づき前記コンテンツ復号化鍵を取得するステップと、前記コンテンツ復号化鍵に基づき前記暗号化コンテンツを復号化するステップと、を含むことを特徴とする。

【発明の効果】

【００２８】

本発明のコンテンツ配信システムによれば、漏洩元の追跡が出来ない全出力装置共通のコンテンツ復号化鍵を埋め込んだ不正な出力装置をすばやく無効化することを目的に、鍵発行センタがコンテンツ暗号化鍵及び対応するコンテンツ復号化鍵を更新したときに、出力装置へ配信するデータサイズの削減を行った。このことによって、限られたデータサイズしか転送出来ない通信路においても、より多くコンテンツ暗号化鍵及びコンテンツ復号化鍵を更新することが出来るため、漏洩元の追跡が不可能なコンテンツ復号化鍵を埋め込んだ不正な出力装置を作成する攻撃に対する耐性が増すことになる。

【発明を実施するための最良の形態】

【００２９】

以下本発明に係るコンテンツ配信システムの実施の形態について、図面を参照しながら説明する。

（実施の形態１）

本発明に係る一つの実施の形態としてのコンテンツ配信システム１について説明する。最初に、図１を用いて本実施の形態の概要を説明する。なお、以後、コンテンツを出力する出力装置が８台の場合について説明を行うが、これは８台以外であっても同様に実現可能である。

【００３０】

図１において、１０は後述する鍵発行センタ１１と後述するサーバ１２と後述する８台の出力装置１３ａ～１３ｈとが接続されている通信路であり、インターネット等のネットワークである。ここで、鍵発行センタ１１と出力装置１３ａ～１３ｈの全ての組には、予め各々の組が共有している一つの個別鍵が与えられているとし、例えば鍵発行センタ１１と出力装置１３ａは個別鍵ＩＫａを、鍵発行センタ１１と出力装置１３ｂは個別鍵ＩＫｂを、鍵発行センタ１１と出力装置１３ｈは個別鍵ＩＫｈを予め共有しているとする。

【００３１】

ここでは、各構成要素の動作について説明する。まず、全ての出力装置１３ａ～１３ｈがコンテンツ復号化鍵を取得する際に用いるノード暗号化鍵及びノード復号化鍵に関する情報を配布する方法について説明する。

鍵発行センタ１１は事前準備として、まず、例えば図２で示すような一つのノードが２つの子ノードを持つ２分木で深さが３の木構造を１つ用意し、サーバ１２と共有しておく。なお、本発明で使用する木構造はＮ分木（Ｎは３以上の自然数）であっても、深さがＭ（Ｍは２以上の自然数）であっても良く、複数の木構造を利用しても良い。これ以降、本発明で使用する木構造において、ルートノードの深さ（階層）を第０階層、ルートノード（第０階層）の子ノードの深さを第１階層、その第１階層のノードの子ノードの深さを第２階層、その第２階層のノードの子ノードの深さを第３階層と呼ぶ。そして、全ノードの名前付けとして、ルートノードを第０ノード、第０ノードの２つの子ノードのうち１つを

第１ノード、もう一方を第２ノードとする。また、第１ノードの２つの子ノードを第３ノードと第４ノードとし、第２ノードの２つの子ノードを第５ノードと第６ノードとする。さらに、第３ノードの２つの子ノードを第７ノードと第８ノードとし、第４ノードの２つの子ノードを第９ノードと第１０ノードとし、第５ノードの２つの子ノードを第１１ノードと第１２ノードとし、第６ノードの２つの子ノードを第１３ノードと第１４ノードとする。つまり、今回使用する木構造は全部で１５個のノードから構成される。そして第０ノードには第０ノード暗号化鍵ＮＥＫ０と対応する第０ノード復号化鍵ＮＤＫ０のペアを、第１ノードには第１ノード暗号化鍵ＮＥＫ１と対応する第１ノード復号化鍵ＮＤＫ１のペアを、・・・、第１４ノードには第１４ノード暗号化鍵ＮＥＫ１４及び対応する第１４ノード復号化鍵ＮＤＫ１４のペアをそれぞれランダムに作成し、設定する。ここで、各々の第０ノード復号化鍵ＮＤＫ０から第１４ノード復号化鍵ＮＤＫ１４は、各々の第０ノード暗号化鍵ＮＥＫ０から第１４ノード暗号化鍵１４に対応する復号化鍵であるとし、また、第０ノード復号化鍵ＮＤＫ０から第１４ノード復号化鍵ＮＤＫ１４のそれぞれは各々異なる値になるように設定する。そして第０ノード暗号化鍵ＮＥＫ０から第１４ノード暗号化鍵ＮＥＫ１４により構成される図３で示すような暗号化ノード鍵群ＡＬＬＮＥＫ＝ＮＥＫ０｜｜ＮＥＫ１｜｜・・・｜｜ＮＥＫ１４をサーバ１２へ送信する。また次に、各出力装置１３ａ～１３ｈを、第３階層の各ノードである末端ノードのそれぞれに一つずつ対応付ける。なお、末端ノードには、複数の出力装置を対応付けても良い。そして、各出力装置１３ａ～１３ｈには、末端ノードからルートノードまで辿っていった時に通過する計４つのノード復号化鍵を割り当てる。例えば図２のような木構造の場合、出力装置１３ａには、第０ノード復号化鍵ＮＤＫ０と第１ノード復号化鍵ＮＤＫ１と第３ノード復号化鍵ＮＤＫ３と第７ノード復号化鍵ＮＤＫ７を、出力装置１３ｆには、第０ノード復号化鍵ＮＤＫ０と第２ノード復号化鍵ＮＤＫ２と第５ノード復号化鍵ＮＤＫ５と第１２ノード復号化鍵ＮＤＫ１２を割り当てる。そして、各出力装置１３ａ～１３ｈそれぞれに割り当てられた４つのノード復号化鍵を連結したものを、各々の出力装置と予め共有している個別鍵ＩＫａ～ＩＫｈを用いて暗号化する。例えば、出力装置１３ａに対しては、暗号文Ｅｎｃ（ＩＫａ、ＮＤＫ０｜｜ＮＤＫ１｜｜ＮＤＫ３｜｜ＮＤＫ７）、出力装置１３ｆに対しては、暗号文Ｅｎｃ（ＩＫｆ、ＮＤＫ０｜｜ＮＤＫ２｜｜ＮＤＫ５｜｜ＮＤＫ１２）となる。そして、各々の暗号文を連結したものを鍵更新情報ＵＰＤＫＥＹ＝Ｅｎｃ（ＩＫａ、ＮＤＫ０｜｜ＮＤＫ１｜｜ＮＤＫ３｜｜ＮＤＫ７）｜｜・・・｜｜Ｅｎｃ（ＩＫｈ、ＮＤＫ０｜｜ＮＤＫ２｜｜ＮＤＫ６｜｜ＮＤＫ１４）として、複数の出力装置１３ａ～１３ｈへ配信する。

【００３２】

次に、サーバ１２がコンテンツ復号化鍵ＣＤＫを出力装置１３ａ～１３ｈへ配信する場合の動作について説明する。サーバ１２は、まず、コンテンツＣＮＴを暗号化、復号化するのに用いるコンテンツ暗号化鍵ＣＥＫ，対応するコンテンツ復号化鍵ＣＤＫをランダムに生成する。次に、そのコンテンツ復号化鍵ＣＤＫを暗号化する際に用いる複数のノード暗号化鍵を以下のような方法でノード暗号化鍵群の中から選定する。まず、木構造の末端ノードに対応付けられているノード暗号化鍵（ＮＥＫ７～ＮＥＫ１４）を一つランダムに選定する。ここでは、コンテンツ暗号化鍵ＣＥＫ，コンテンツ復号化鍵ＣＤＫを更新する毎に選定する末端ノード（第７ノード～第１４ノード）を変更する点に注意する。そして、選定したノード暗号化鍵に対応するノード復号化鍵が割り当てられていない出力装置１３ａ～１３ｈが保有しているノード復号化鍵に対応するノード暗号化鍵を選定することを繰り返す。なお、選定済みのノード暗号化鍵に対応するノード復号化鍵が割り当てられていない出力装置１３ａ～１３ｈが存在しなくなるまで繰り返しても良い。上記のような方法により、ノード暗号化鍵群からコンテンツ復号化鍵ＣＤＫを暗号化する際に用いる複数のノード暗号化鍵を選定する。例えば、出力装置１３ａは第７ノード復号化鍵ＮＤＫ７を、出力装置１３ｂは第８ノード復号化鍵ＮＤＫ８を、出力装置１３ｃ～１３ｄは第４ノード復号化鍵ＮＤＫ４を、出力装置１３ｅ～１３ｈは第２ノード復号化鍵ＮＤＫ２をそれぞれ保持しているので、第２ノード暗号化鍵ＮＥＫ２と第４ノード暗号化鍵ＮＥＫ４と第７

ノード暗号化鍵ＮＥＫ７と第８ノード暗号化鍵ＮＥＫ８を選定することはできる。そして、その選定された複数のノード暗号化鍵の各々を用いて、コンテンツ復号化鍵ＣＤＫを暗号化する。例えば、先ほどの例において各暗号文はＥｎｃ（ＮＥＫ２，ＣＤＫ）、Ｅｎｃ（ＮＥＫ４，ＣＤＫ）、Ｅｎｃ（ＮＥＫ７，ＣＤＫ）、Ｅｎｃ（ＮＥＫ８，ＣＤＫ）となる。そして、それら暗号化されたコンテンツ復号化鍵ＣＤＫから構成される暗号化コンテンツ鍵群ＥＮＣＣＤＫＧを出力装置１３ａ～１３ｈへ送信する。例えば、先ほどの例においては、暗号化コンテンツ鍵群ＥＮＣＣＤＫＧ＝Ｅｎｃ（ＮＥＫ２，ＣＤＫ）｜｜Ｅｎｃ（ＮＥＫ４，ＣＤＫ）｜｜Ｅｎｃ（ＮＥＫ７，ＣＤＫ）｜｜Ｅｎｃ（ＮＥＫ８，ＣＤＫ）となる。出力装置１３ａ～１３ｈは、受信した暗号化コンテンツ鍵群ＥＮＣＣＤＫＧから、自身が保有している割当ノード復号化鍵群の中のいずれかのノード復号化鍵に対応している暗号文を探し、その暗号文の復号化を行うことによってコンテンツ復号化鍵ＣＤＫを取得する。例えば、図２のような木構造の場合、出力装置１３ａは第７ノード復号化鍵ＮＤＫ７を保有しているので、第７ノード暗号化鍵ＮＥＫ７を基にしたコンテンツ復号化鍵ＣＤＫの暗号文Ｅｎｃ（ＮＥＫ７、ＣＤＫ）を復号化して、コンテンツ復号化鍵ＣＤＫを取得する。

【００３３】

ここで、サーバ１２はコンテンツ暗号化鍵ＣＥＫ，及び対応するコンテンツ復号化鍵ＣＤＫは更新することを想定し、また、そのコンテンツ復号化鍵ＣＤＫを暗号化する際に用いるノード暗号化鍵群の中から選定する複数のノード暗号化鍵も更新するようにする。

次に、サーバ１２がコンテンツを出力装置１３ａ～１３ｈへ配信する場合の動作について説明する。サーバ１２は、コンテンツ暗号化鍵ＣＥＫに基づいてコンテンツＣＮＴの暗号化を行い、その暗号化コンテンツＥＮＣＣＮＴ＝Ｅｎｃ（ＣＥＫ，ＣＮＴ）を複数の出力装置１３ａ～１３ｈへ向けて配信する。出力装置１３ａ～１３ｈは、暗号化コンテンツＥＮＣＣＮＴを受信し、コンテンツ復号化鍵ＣＤＫに基づいて、暗号化コンテンツＥＮＣＣＮＴの復号化を行い、その復号化コンテンツＤＥＣＣＮＴを外部へ出力する。

【００３４】

なお、本実施の形態であるコンテンツ配信システム１では、鍵発行センタ１１がある特定の個別鍵を持つ出力装置を無効化し、コンテンツＣＮＴを復号化出来ないようにすることも可能となる。これは以下のようにして実現可能である。ここでは、出力装置１３ａを無効化する場合について説明する。鍵発行センタ１１は、外部から出力装置１３ａを識別する出力装置識別子ＡＩＤａを受け取り、全てのノード暗号化鍵及びノード暗号化鍵を新たに生成する。そして、全てのノード暗号化鍵（ＮＥＫ０～ＮＥＫ１４）から成る暗号化ノード鍵群ＡＬＬＮＥＫをサーバ１２へ送信する。また、出力装置１３ａ以外の各出力装置１３ｂ～１３ｈに個別に全てのノード復号化鍵（ＮＤＫ０～ＮＤＫ１４）から４つのノード復号化鍵を割り当て、割り当てられた４つのノード復号化鍵から構成される割当ノード復号化鍵群（ＡＮＤＫＧｂ～ＡＮＤＫＧｈ）を作成する。そして、出力装置識別子ＡＩＤａに対応する出力装置１３ａ以外のそれぞれの出力装置１３ｂ～１３ｈが持つ個別鍵ＩＫｂ～ＩＫｈに基づいて、それぞれの割当ノード復号化鍵群ＡＮＤＫＧＧｂ～ＡＮＤＫＧｈの暗号化を行う。そしてその暗号文を連結した値を暗号化コンテンツ鍵群ＥＮＣＣＤＫＧとして複数の出力装置１３ａ～１３ｈへ向けて配信する。そうすることにより、その鍵発行センタ１１に入力された出力装置識別子ＡＩＤａに対応する出力装置１３ａでは、暗号化コンテンツ鍵ＥＮＣＣＤＫＧの中に個別鍵ＩＫａに対応する割当ノード復号化鍵群の暗号文がないので、新たに４つのノード復号化鍵を取得出来なくなり、その結果コンテンツ復号化鍵ＣＤＫを生成出来なくなる。つまり、暗号化コンテンツＥＮＣＣＮＴ＝Ｅｎｃ（ＣＤＫ，ＣＮＴ）を復号化出来なくなるので、その出力装置１３ａの無効化を実現出来る。なお、出力装置１３ａ以外の出力装置１３ｂ～１３ｈを無効化する場合も、出力装置１３ａと同様の動作を行うが、持っている個別鍵は出力装置毎に異なるため、割当ノード復号化鍵の各々を暗号化する個別鍵が違う点が異なる。以上のようにして、鍵発行センタ１１はある特定の個別鍵を有する出力装置の無効化が実現することが出来る。

【００３５】

以上が、本実施の形態の概要である。以下に、本発明のコンテンツ配信システムの一実施形態であるコンテンツ配信システム１の詳細について説明を行う。これらの構成要素について詳細に説明する。

＜コンテンツ配信システム１の構成＞

コンテンツ配信システム１は、図１に示すように、通信路１０と、鍵発行センタ１１と、サーバ１２と、複数の出力装置１３ａ～１３ｈから構成される。

【００３６】

鍵発行センタ１１はコンテンツ復号化鍵ＣＤＫを暗号化するのに用いるノード暗号化鍵群ＡＬＬＮＥＫをサーバ１２へ送信する。また、コンテンツ復号化鍵ＣＤＫを取得する際に用いるノード復号化鍵（ＮＤＫ０～ＮＤＫ１４）のいずれか４つを、図２で示すような木構造を用いて、各々の出力装置１３ａ～１３ｈに個別に割り当てる。そして、その各出力装置１３ａ～１３ｈに割り当てられたそれぞれ４つのノード復号化鍵を連結したものを各出力装置の持つ個別鍵ＩＫａ～ＩＫｈを用いて暗号化する。その暗号文を結合した値を鍵更新情報ＵＰＤＫＥＹとして複数の出力装置１３ａ～１３ｈへ配信する。出力装置１３ａ～１３ｈは、鍵更新情報ＵＰＤＫＥＹの中から、自身が持つ個別鍵ＩＫａ～ＩＫｈに対応する暗号文を取得し、その暗号文を個別鍵を用いて復号化することによって、自身の出力装置に割り当てられた４つのノード復号化鍵を取得する。サーバ１２は、コンテンツＣＮＴを暗号化、復号化するコンテンツ暗号化鍵ＣＥＫ，コンテンツ復号化鍵ＣＤＫを作成し、そのコンテンツ復号化鍵ＣＤＫを暗号化する際に用いる複数のノード暗号化鍵を以下のような方法でノード暗号化鍵群の中から選定する。まず、木構造の末端ノードに対応付けられているノード暗号化鍵（ＮＥＫ７～ＮＥＫ１４）を一つランダムに選定する。ここでは、コンテンツ暗号化鍵ＣＥＫ，コンテンツ復号化鍵ＣＤＫを更新する毎に選定する末端ノード（第７ノード～第１４ノード）を変更する点に注意する。そして、選定したノード暗号化鍵に対応するノード復号化鍵が割り当てられていない出力装置１３ａ～１３ｈが保有しているノード復号化鍵に対応するノード暗号化鍵を選定することを繰り返す。上記のような方法により、ノード暗号化鍵群からコンテンツ復号化鍵ＣＤＫを暗号化する際に用いる複数のノード暗号化鍵を選定する。そして、その選定された複数のノード暗号化鍵それぞれを用いて、コンテンツ復号化鍵ＣＤＫの暗号化を行い、その暗号文を連結したものを暗号化コンテンツ鍵群ＥＮＣＣＤＫＧとして出力装置１３ａ～１３ｈへ送信する。そして、出力装置１３ａ～１３ｈは、自身の保有する割当ノード復号化鍵の中の４つのノード復号化鍵のいずれかを用いて、暗号化コンテンツ鍵群ＥＮＣＣＤＫＧの中の対応するコンテンツ復号化鍵の暗号文を復号化して、コンテンツ復号化鍵ＣＤＫを取得する。サーバ１２はコンテンツＣＮＴを暗号化して暗号化コンテンツＥＮＣＣＮＴ＝Ｅｎｃ（ＣＥＫ，ＣＮＴ）として出力装置１３ａ～１３ｈへ配信し、出力装置１３ａ～１３ｈはコンテンツ復号化鍵ＣＤＫに基づき、受信した暗号化コンテンツＥＮＣＣＮＴの復号化を行い、その復号化コンテンツＤＥＣＣＮＴを外部へ出力する。

【００３７】

以下に、これらの構成要素について詳細に説明する。まず、通信路１０の構成について述べ、続いて鍵発行センタ１１及びサーバ１２及び複数の出力装置１３ａ～１３ｈの構成と動作について図を用いて説明する。

＜通信路１０の構成＞

通信路は、例えば、インターネット、電話回線や専用線等のようなネットワークである。

【００３８】

＜鍵発行センタ１１の構成＞

鍵発行センタ１１は、図４に示すように、ノード鍵生成部１１１、第一送信部１１２、出力装置対応情報格納部１１３、第一暗号化部１１４、第二送信部１１５、入力部１１６、対応情報更新部１１７から構成される。

（１）ノード鍵生成部１１１

ノード鍵生成部１１１は、予めノード鍵更新条件が与えられており、そのノード鍵更新

条件を満たした場合、もしくは、後述する対応情報更新部１１７からノード鍵生成要求ＲＥＱ１を受信した場合、もしくは、鍵発行センタ１１が動作を開始した場合、ノード鍵生成部１１１は、まず第０ノード暗号化鍵ＮＥＫ０と対応する第０ノード復号化鍵ＮＤＫ０のペア、第１ノード暗号化鍵ＮＥＫ１と対応する第１ノード復号化鍵ＮＤＫ１のペア、・・・、第１４ノード暗号化鍵ＮＥＫ１４と対応する第１４ノード復号化鍵ＮＤＫ１４のペアの計１５ペアをそれぞれランダムに作成する。ここで、各ノード暗号化鍵及びノード復号化鍵は、例えばＡＥＳ暗号方式の１２８ビット鍵などである。そして、各ノード暗号化鍵（ＮＥＫ０～ＮＥＫ１４）を連結したものから構成される図３で示すようなノード暗号化鍵群ＡＬＬＮＥＫ＝ＮＥＫ０｜｜ＮＥＫ１｜｜・・・｜｜ＮＥＫ１４を作成し、そのノード暗号化鍵群ＡＬＬＮＥＫを第一送信部１１２に出力する。次に、例えば、図２のような木構造の場合、８つの末端ノード（第７ノード～第１４ノード）の各ノードに出力装置１３ａ～１３ｈをそれぞれ対応付け、そして、各出力装置１３ａ～１３ｈに対応付けられた末端ノードからルートノードに辿っていった時に通過する４つのノード復号化鍵を割り当てる。例えば、図２のような木構造の場合、出力装置１３ａには、第０ノード復号化鍵ＮＤＫ０と第１ノード復号化鍵ＮＤＫ１と第３ノード復号化鍵ＮＤＫ３と第７ノード復号化鍵ＮＤＫ７を割り当て、出力装置１３ｆには、第０ノード復号化鍵ＮＤＫ０と第２ノードＮＤＫ２と第５ノード復号化鍵ＮＤＫ５と第１２ノード復号化鍵ＮＤＫ１２を割り当てる。そして、各出力装置１３ａ～１３ｈのそれぞれに割り当てられた４つのノード復号化鍵から構成される割当ノード復号化鍵群ＡＮＤＫＧａ～ＡＮＤＫＧｈを作成する。例えば、図５が示すように出力装置１３ａ向けの割当ノード復号化鍵群はＡＮＤＫＧａ＝ＮＤＫ０｜｜ＮＤＫ１｜｜ＮＤＫ３｜｜ＮＤＫ７であり、出力装置１３ｆ向けの割当ノード復号化鍵群はＡＮＤＫＧｆ＝ＮＤＫ０｜｜ＮＤＫ２｜｜ＮＤＫ５｜｜ＮＤＫ１２である。そして、その生成した割当ノード復号化鍵群ＡＮＤＫＧａ～ＡＮＤＫＧｈのそれぞれを各々の出力装置識別子ＡＩＤａ～ＡＩＤｈに対応付けて、図６で示すような出力装置対応情報格納部１１３へ格納する。そして最後に、鍵更新情報生成要求ＲＥＱ２を第一暗号化部１１４へ出力する。なお、ノード鍵生成部１１１に予め与えられるノード鍵更新条件は、例えば、”１年毎”などであり、これはノード鍵生成部１１１がカウンタを保持することで実現出来る。

【００３９】

（２）第一送信部１１２

第一送信部１１２は、ノード鍵生成部１１１から受け取ったノード暗号化鍵群ＡＬＬＮＥＫを通信路１０を経由してサーバ１２に送信するものである。

（３）出力装置対応情報格納部１１３

出力装置対応情報格納部１１３は、図６で示すように、出力装置１３ａ～１３ｈを識別する複数の出力装置識別子ＡＩＤａ～ＡＩＤｈと、その各出力装置１３ａ～１３ｈに予め与えられている複数の個別鍵ＩＫａ～ＩＫｈ及び割当ノード復号化鍵群ＡＮＤＫＧａ～ＡＮＤＫＧｈを保持するものである。例えば、図６においては、出力装置識別子ＡＩＤａに対応づけられている出力装置１３ａは個別鍵ＩＫａと割当ノード復号化鍵群ＡＮＤＫＧａを保持し、出力装置識別子ＡＩＤｂに対応づけられている出力装置１３ｂは個別鍵ＩＫｂ及び割当ノード復号化鍵群ＡＮＤＫＧｂを保持し、出力装置識別子ＡＩＤｈに対応づけられている出力装置１３ｈは個別鍵ＩＫｈ及び割当ノード復号化鍵群ＡＮＤＫＧｈを保持していることを表している。出力装置情報格納部１１３へは、ノード鍵生成部１１１及び第一暗号化部１１４及び対応情報更新部１１７からアクセス可能である。

【００４０】

（４）第一暗号化部１１４

第一暗号化部１１４は、ノード鍵生成部１１１から鍵更新情報生成要求ＲＥＱ２を受け取った場合、出力装置対応情報格納部１１３にアクセスして、複数の出力装置識別子ＡＩＤａ～ＡＩＤｈ及び個別鍵ＩＫａ～ＩＫｈ及び割当ノード復号化鍵群ＡＮＤＫＧａ～ＡＮＤＫＧｈを全て取得する。そして、まず、出力装置識別子ＡＩＤａに対して、対応している個別鍵ＩＫａに基づいて割当ノード復号化鍵群ＡＮＤＫＧａの暗号化を行い、その暗号

文を暗号化割当ノード復号化鍵群ＥＮＣＡＮＤＫＧａ＝Ｅｎｃ（ＩＫａ，ＡＮＤＫＧａ）として、出力装置識別子ＡＩＤａに対応付ける。続いて、他の出力装置識別子ＡＩＤｂ～ＡＩＤｈに対しても、同様に、対応づけられている個別鍵に基づいて対応付けられている割当ノード復号化鍵群の暗号化を行い、その暗号文Ｅｎｃ（ＩＫｂ，ＡＮＤＫＧｂ）、・・・、Ｅｎｃ（ＩＫｎ，ＡＮＤＫＧｈ）を暗号化割当ノード復号化鍵群ＥＮＣＡＮＤＫＧｂ、・・・、ＥＮＣＡＮＤＫＧｈとし、それぞれの出力装置識別子ＡＩＤｂ～ＡＩＤｈに対応付ける。そして、図７で示すような、複数の出力装置識別子ＡＩＤａ～ＡＩＤｈ及び暗号化割当ノード復号化鍵群ＥＮＣＡＮＤＫＧａ～ＥＮＣＡＮＤＫＧｈから構成される鍵更新情報ＵＰＤＫＥＹ＝｛ＡＩＤａ，ＥＮＣＡＮＤＫＧａ｝｜｜｛ＡＩＤｂ，ＥＮＣＡＮＤＫＧｂ｝・・・｜｜｛ＡＩＤｈ，ＥＮＣＡＮＤＫＧｈ｝｝を生成し、その鍵更新情報ＵＰＤＫＥＹを第二送信部１１５に出力する。ここで割当ノード復号化鍵群を暗号化するのに使用する暗号化アルゴリズムは、例えば、ブロック暗号のＡＥＳ方式やＤＥＳ方式などであり、各出力装置１３ａ～１３ｈのそれぞれの第二復号化部１３８ａで用いる復号化アルゴリズムと同じ方式を用いる。

【００４１】

（５）第二送信部１１５

第二送信部１１５は、第一暗号化部１１４から鍵更新情報ＵＰＤＫＥＹを受信した場合、受信した鍵更新情報ＵＰＤＫＥＹを通信路１０を経由して複数の出力装置１３ａ～１３ｈに配信する。

（６）入力部１１６

入力部１１６は、外部から出力装置１３ａ～１３ｈのいずれかを識別する出力装置識別子ＡＩＤａ～ＡＩＤｈのいずれかを入力出来るものであり、外部から出力装置識別子ＡＩＤａ～ＡＩＤｈのいずれかを受信した場合、対応情報更新部１１７にその受信した出力装置識別子を出力する。なお、入力部１１６は、鍵発行センタ１１がある特定の個別鍵を有する出力装置の無効化を行う際に、どの出力装置を無効化するのかを判別するために利用するものなので、鍵発行センタ１１が出力装置の無効化を行わない場合は、入力部１１６が鍵発行センタ１１の中に存在していなくても良い。

【００４２】

（７）対応情報更新部１１７

対応情報更新部１１７は、入力部１１６から出力装置識別子ＡＩＤａ～ＡＩＤｈのいずれかを受信した場合、まず図６で示すような出力装置対応情報格納部１１３にアクセスし、その中から受信した出力装置識別子及びその出力装置識別子に対応付けられている個別鍵及び割当ノード復号化鍵群を出力装置対応情報格納部１１３から削除する。例えば、図６のような出力装置対応情報格納部１１３において、対応情報更新部１１７が出力装置識別子ＡＩＤａを受信したとすると、対応する出力装置識別子ＡＩＤａ及び個別鍵ＩＫａ及び割当ノード復号化鍵群ＡＮＤＫＧａを出力装置対応情報格納部１１３から削除することで、図８のようになる。削除が終わったら、ノード鍵生成部１１１にノード鍵生成要求ＲＥＱ１を出力する。なお、対応情報更新部１１７は、鍵発行センタ１１がある特定の個別鍵を有する出力装置の無効化を行う際に利用するものであるため、鍵発行センタ１１が出力装置の無効化を行わない場合は、対応情報更新部１１７が鍵発行センタ１１の中に存在していなくても良い。

【００４３】

＜鍵発行センタ１１の動作＞

以上で、鍵発行センタ１１の構成について説明を行ったが、ここでは鍵発行センタ１１の動作について説明する。まず、予め与えられるノード鍵更新条件を満たした場合、もしくは、鍵発行センタ１１が動作を開始した場合などにおいて、複数のノード暗号化鍵及びノード復号化鍵を更新する場合の動作について図９に示すフローチャートを用いて説明する。また、鍵発行センタ１１は入力部１１６及び対応情報更新部１１７も構成要素とすることによって、ある特定の個別鍵を有する出力装置を無効化する機能を持たせることも可能であるが、ここでは具体例として、出力装置１３ａを無効化する時の動作について図１

０に示すフローチャートを用いて説明する。

【００４４】

≪ノード暗号化鍵及びノード復号化鍵の更新時の動作≫

ノード鍵生成部１１１は、第０ノード暗号化鍵ＮＥＫ０と対応する第０ノード復号化鍵ＮＤＫ０、・・・、第１４ノード暗号化鍵ＮＥＫ１４と対応する第１４ノード復号化鍵ＮＤＫ１４の計１５ペアをランダムに作成する（Ｓ１１０１）。

ノード鍵生成部１１１は、図３で示すような、第０ノード暗号化鍵ＮＥＫ０から第１４ノード暗号化鍵ＮＥＫ１４の計１５個のノード暗号化鍵から構成されるノード暗号化鍵群ＡＬＬＮＥＫを作成する（Ｓ１１０２）。

【００４５】

ノード鍵生成部１１１は、ノード暗号化鍵群ＡＬＬＮＥＫを、第一送信部１１２へ出力する（Ｓ１１０３）。

第一送信部１１２は、受信したノード暗号化鍵群ＡＬＬＮＥＫを、サーバ１２へ向けて送信する（Ｓ１１０４）。

ノード鍵生成部１１１は、出力装置対応情報格納部１１３に格納されている割当ノード復号化鍵群ＡＮＤＫＧａ～ＡＮＤＫＧｈを全て削除する。また、図２で示すような予め与えられる木構造に対して、８つの末端ノードの各ノードに出力装置１３ａ～１３ｈを一つずつそれぞれ対応付ける（Ｓ１１０５）。

【００４６】

ノード鍵生成部１１１は、まだ割当ノード復号化鍵群を生成していない出力装置に対して、対応付けられている末端ノードからルートノードまで辿っていった時に通過する４つのノード復号化鍵から構成される割当ノード復号化鍵群を作成する。そして、その割当ノード復号化鍵群を出力装置識別子に対応づけて、出力装置対応情報格納部１１３へ格納する（Ｓ１１０６）。

【００４７】

もし、出力装置対応情報格納部１１３の中にある全ての出力装置識別子ＡＩＤａ～ＡＩＤｈに対して割当ノード復号化鍵群ＡＮＤＫＧａ～ＡＮＤＫＧｈを割り当てられたら、ステップＳ１１０８へ進む。もし、残っていたらステップＳ１１０６に戻る（Ｓ１１０７）。

ノード鍵生成部１１１は、鍵更新情報生成要求ＲＥＱ２を第一暗号化部１１４へ出力する（Ｓ１１０８）。

【００４８】

鍵更新情報生成要求ＲＥＱ２を受け取った第一暗号化部１１４は、出力装置対応情報格納部１１３にアクセスして、出力装置識別子ＡＩＤａ～ＡＩＤｈ及び個別鍵ＩＫａ～ＩＫｈ及び割当ノード復号化鍵群ＡＮＤＫＧａ～ＡＮＤＫＧｈをそれぞれ全て取得する（Ｓ１１０９）。

暗号化部１１５は、各々の個別鍵ＩＫａ～ＩＫｈに基づいて、各々の割当ノード復号化鍵群ＡＮＤＫＧａ～ＡＮＤＫＧｈを暗号化し、その暗号化された割当ノード復号化鍵群ＥＮＣＡＮＤＫＧａ～ＥＮＣＡＮＤＫＧｈ及び暗号化に用いた個別鍵ＩＫａ～ＩＫｈに対応する出力装置識別子ＡＩＤａ～ＡＩＤｈのそれぞれから構成される鍵更新情報ＵＰＤＫＥＹを生成する（Ｓ１１１０）。

【００４９】

第一暗号化部１１４は、生成した鍵更新情報ＵＰＤＫＥＹを第二送信部１１５に出力する（Ｓ１１１１）。

第二送信部１１５は、鍵更新情報ＵＰＤＫＥＹを受け取り、その受信した鍵更新情報ＵＰＤＫＥＹを複数の出力装置１３ａ～１３ｈへ向けて配信し、終了する（Ｓ１１１２）。

≪出力装置１３ａの無効化時の動作≫

入力部１１６は、受信した出力装置識別子ＡＩＤａを、対応情報更新部１１７へ出力する（Ｓ１１５１）。

【００５０】

対応情報更新部１１７は、入力部１１６から受信した出力装置識別子ＡＩＤａ及びその出力装置識別子ＡＩＤａに対応する個別鍵ＩＫａと割当ノード復号化鍵群ＡＮＤＫＧａを出力装置対応情報格納部１１３から削除する（Ｓ１１５２）。

対応情報更新部１１７は、ノード鍵生成部１１１へノード鍵生成要求ＲＥＱ１を出力し、ステップＳ１１０１に進む（Ｓ１１５３）。

【００５１】

なお、出力装置１３ａ以外の出力装置１３ｂ～１３ｈのいずれかを無効化する時の動作も、出力装置１３ａの場合とほぼ同様の動作となるが、対応情報更新部１１７において、出力装置対応情報格納部１１３から削除する出力装置識別子及び個別鍵及び割当ノード復号化鍵群が無効化する出力装置１３ｂ～１３ｈに依存して変化する点が異なる。

以上が、コンテンツ配信システム１の構成要素である鍵発行センタ１１の構成と動作である。続いて、サーバ１２の構成と動作について説明を行う。

【００５２】

＜サーバ１２の構成＞

サーバ１２は、図１０に示すように、入力部１２１、暗号化部１２２、鍵情報格納部１２３、コンテンツ鍵選択部１２４、送信部１２５、受信部１２６、コンテンツ鍵生成部１２７から構成される。

（１）入力部１２１

入力部１２１は、外部からコンテンツＣＮＴを入力できるものである。外部から入力されるコンテンツＣＮＴは、複数の出力装置１３ａ～１３ｈで出力可能なフォーマット形式であって、例えば、ＭＰＥＧフォーマットによる動画データやＭＰ３フォーマットによる音声データなどである。入力部１２１は、外部からコンテンツＣＮＴを受信した場合、その受信したコンテンツＣＮＴを暗号化部１２２に出力する。

【００５３】

（２）暗号化部１２２

暗号化部１２２は、入力部１２１からコンテンツＣＮＴを受信した場合、図１２に示すような鍵情報格納部１２３にアクセスして、コンテンツ暗号化鍵ＣＥＫを取得し、取得したコンテンツ暗号化鍵ＣＥＫに基づいて、逐次、入力部１２１から受け取ったコンテンツＣＮＴの暗号化を行う。ここでコンテンツＣＮＴの暗号化に使用する暗号アルゴリズムは、例えば、ブロック暗号のＡＥＳ方式やＤＥＳ方式などであり、後述する複数の出力装置１３ａ～１３ｈのそれぞれの第一復号化部１３５において暗号化コンテンツＥＮＣＣＮＴを復号化するのに用いるアルゴリズムと同じ方式を用いる。その後、暗号化されたコンテンツＥＮＣＣＮＴをコンテンツ鍵選択部１２４に出力する。

【００５４】

（３）鍵情報格納部１２３

鍵情報格納部１２３は、図１２で示すように、コンテンツ暗号化鍵ＣＥＫ及びコンテンツ復号化鍵ＣＤＫ及びノード暗号化鍵群ＡＬＬＮＥＫ及びノード復号化鍵群ＡＬＬＮＤＫが格納されている。

（４）コンテンツ鍵選択部１２４

コンテンツ鍵選択部１２４は、暗号化部１２２から暗号化コンテンツＥＮＣＣＮＴを受信した場合、鍵情報格納部１２３にアクセスして、コンテンツ復号化鍵ＣＤＫ及びノード暗号化鍵群ＡＬＬＮＥＫを取得する。そして、そのコンテンツ復号化鍵ＣＤＫを暗号化する際に用いるノード暗号化鍵群ＡＬＬＮＥＫの中の複数のノード暗号化鍵（ＮＥＫ０～ＮＥＫ１４）を以下のような方法で選定する。まず、木構造の末端ノードに対応付けられているノード暗号化鍵（ＮＥＫ７～ＮＥＫ１４）を一つランダムに選定する。ここでは、コンテンツ暗号化鍵ＣＥＫ，コンテンツ復号化鍵ＣＤＫを更新する毎に選定する末端ノード（第７ノード～第１４ノード）を変更する点に注意する。そして、選定したノード暗号化鍵に対応するノード復号化鍵が割り当てられていない出力装置１３ａ～１３ｈが保有しているノード復号化鍵に対応するノード暗号化鍵を選定することを繰り返す。上記のような方法により、ノード暗号化鍵群からコンテンツ復号化鍵ＣＤＫを暗号化する際に用いる複

数のノード暗号化鍵を選定する。そして、その選定された複数のノード暗号化鍵それぞれを用いて、コンテンツ復号化鍵ＣＤＫの暗号化を行う。例えば、出力装置１３ａは第７ノード復号化鍵ＮＤＫ７を、出力装置１３ｂは第８ノード復号化鍵ＮＤＫ８を、出力装置１３ｃ～１３ｄは第４ノード復号化鍵ＮＤＫ４を、出力装置１３ｅ～１３ｈは第２ノード復号化鍵ＮＤＫ２をそれぞれ保持しているので、暗号化第２ノード復号化鍵ＥＮＣＮＤＫ２＝Ｅｎｃ（ＮＤＫ２，ＣＤＫ）と暗号化第４ノード復号化鍵ＥＮＣＮＤＫ４＝Ｅｎｃ（ＮＤＫ４，ＣＤＫ）と暗号化第７ノード復号化鍵ＥＮＣＮＤＫ７＝Ｅｎｃ（ＮＤＫ７，ＣＤＫ）と暗号化第８ノード復号化鍵ＥＮＣＮＤＫ８＝Ｅｎｃ（ＮＤＫ８，ＣＤＫ）は選定可能である。そして、それら複数の暗号化ノード復号化鍵から成る図１４で示すような暗号化コンテンツ鍵群ＥＮＣＣＤＫＧを生成し、受信した暗号化コンテンツＥＮＣＣＮＴとその暗号化コンテンツ鍵群ＥＮＣＣＤＫＧを送信部１２５へ出力する。例えば、複数のノード暗号化鍵としてＮＥＫ２とＮＥＫ４とＮＥＫ７とＮＥＫ８を選定した場合、ＥＮＣＣＤＫＧ＝Ｅｎｃ（ＮＥＫ２，ＣＤＫ）｜｜Ｅｎｃ（ＮＥＫ４，ＣＤＫ）｜｜Ｅｎｃ（ＮＥＫ７，ＣＤＫ）｜｜Ｅｎｃ（ＮＥＫ８，ＣＤＫ）となる。

【００５５】

（５）送信部１２５

送信部１２５は、逐次、コンテンツ鍵選択部１２４から受け取った暗号化コンテンツＥＮＣＣＮＴ及び暗号化コンテンツ鍵群ＥＮＣＣＤＫＧを、通信路１０を経由して複数の出力装置１３ａ～１３ｈに配信する。

（６）受信部１２６

受信部１２６が、鍵発行センタ１１からノード暗号化鍵群ＡＬＬＮＥＫを受信した場合、受信したノード暗号化鍵群ＡＬＬＮＥＫを鍵情報格納部１２３に格納する。

【００５６】

（７）コンテンツ鍵生成部１２７

コンテンツ鍵生成部１２７には、予めコンテンツ鍵更新条件が与えられており、その条件を満たした場合に、コンテンツ暗号化鍵ＣＥＫ及び対応するコンテンツ復号化鍵ＣＤＫのペアをランダムに生成する。例えば、コンテンツ暗号化鍵ＣＥＫ及びコンテンツ復号化鍵ＣＤＫはＡＥＳ方式の１２８ビット鍵である。そして、コンテンツ暗号化鍵ＣＥＫ及びコンテンツ復号化鍵ＣＤＫを鍵情報格納部１２３へ格納する。なお、コンテンツ鍵生成部１２７に予め与えられるコンテンツ鍵更新条件は、例えば、”１分毎”などであり、これはコンテンツ鍵生成部１２７がカウンタを保持することで実現出来る。

【００５７】

＜サーバ１２の動作＞

以上で、サーバ１２の構成について説明を行ったが、ここでサーバ１２の動作について説明する。まず、コンテンツ配信時の動作について図１５に示すフローチャートを用いて説明する。そして、ノード暗号化鍵群ＡＬＬＮＥＫを受信する場合の動作について図１６に示すフローチャートを用いて説明する。最後に、コンテンツ暗号化鍵ＣＥＫ、コンテンツ復号化鍵ＣＤＫを更新する時の動作について図１７に示すフローチャートを用いて説明する。

【００５８】

≪コンテンツＣＮＴの配信時の動作≫

受信部１２１が、外部からコンテンツＣＮＴを受け取った場合、ステップＳ１２０２に進む。受信していない場合、終了する（Ｓ１２０１）。

受信部１２１は、受信したコンテンツＣＮＴを暗号化部１２２に出力する（Ｓ１２０２）。

【００５９】

コンテンツＣＮＴを受信した第一暗号化部１２２は、鍵情報格納部１１３にアクセスして、コンテンツ暗号化鍵ＣＥＫを取得する（Ｓ１２０３）。

第一暗号化部１２２は、コンテンツ暗号化鍵ＣＥＫに基づいてコンテンツＣＮＴの暗号化を行い、その暗号化コンテンツＥＮＣＣＮＴをコンテンツ鍵選択部１２４へ出力する（

Ｓ１２０４）。

【００６０】

暗号化コンテンツＥＮＣＣＮＴを受け取ったコンテンツ鍵選択部１２４は、鍵情報格納部１２３にアクセスして、ノード暗号化群ＡＬＬＮＥＫ及びコンテンツ復号化鍵ＣＤＫを取得する（Ｓ１２０５）。

コンテンツ鍵選択部１２４は、木構造の末端ノードに対応付けられているノード暗号化鍵（ＮＥＫ７～ＮＥＫ１４）を一つランダムに選定し、そして、選定したノード暗号化鍵に対応するノード復号化鍵が割り当てられていない出力装置１３ａ～１３ｈが保有しているノード復号化鍵に対応するノード暗号化鍵を選定することを繰り返す。上記のような方法により、ノード暗号化鍵群からコンテンツ復号化鍵ＣＤＫを暗号化する際に用いる複数のノード暗号化鍵を選定し、その選定された複数のノード暗号化鍵それぞれを用いて、コンテンツ復号化鍵ＣＤＫの暗号化を行う。そして、それら複数の暗号文から構成される暗号化コンテンツ鍵群ＥＮＣＣＤＫＧを生成する（Ｓ１２０６）。

【００６１】

コンテンツ鍵選択部１２４は、暗号化コンテンツ鍵群ＥＮＣＣＤＫＧと暗号化コンテンツＥＮＣＣＮＴを、送信部１２５へ出力する（Ｓ１２０７）。

暗号化コンテンツＥＮＣＣＮＴ及び暗号化コンテンツ鍵群ＥＮＣＣＤＫを受け取った送信部１２５は、その暗号化コンテンツＥＮＣＣＮＴ及び暗号化コンテンツ鍵群ＥＮＣＣＤＫを出力装置１３ａ～１３ｈへ向けて配信し、終了する（Ｓ１２０８）。

【００６２】

≪ノード暗号化鍵群受信時の動作≫

受信部１２６が、鍵発行センタ１１からノード暗号化鍵群ＡＬＬＮＥＫを受け取った場合、ステップＳ１２３２に進む。受信していない場合、終了する（Ｓ１２３１）。

受信部１２６は、受信したノード暗号化鍵群ＡＬＬＮＥＫを鍵情報格納部１２３へ格納する。終了する（Ｓ１２３２）。

【００６３】

≪コンテンツ暗号化鍵、コンテンツ復号化鍵更新時の動作≫

コンテンツ鍵生成部１２７は、予め与えられたコンテンツ鍵更新条件を満たしている場合、ステップＳ１２６２に進む。コンテンツ鍵更新条件を満たしていない場合、終了する（Ｓ１２６１）。

コンテンツ鍵生成部１２７は、コンテンツ暗号化鍵ＣＥＫ及び対応するコンテンツ復号化鍵ＣＤＫのペアをランダムに生成する（Ｓ１２６２）。

【００６４】

コンテンツ鍵生成部１２７は、コンテンツ暗号化鍵ＣＥＫ及びコンテンツ復号化鍵ＣＤＫを鍵情報格納部１２３へ格納し、終了する（Ｓ１２６３）。

以上が、コンテンツ配信システム１の構成要素であるサーバ１２の構成と動作である。続いて、出力装置１３ａ～１３ｈの構成と動作について説明を行う。まず、出力装置１３ａの構成と動作について説明を行い、次に、出力装置１３ａと他の出力装置１３ｂ～１３ｈと異なる点について述べる。

【００６５】

＜出力装置１３ａの構成＞

出力装置１３ａは、図１８に示すように、第一受信部１３１、復号化鍵取得部１３２ａ、ノード鍵格納部１３３ａ、第一復号化部１３４、出力部１３５、第二受信部１３６、第二復号化部１３７ａ、個別鍵格納部１３８ａから構成される。ここで、第一受信部１３１、第一復号化部１３４、出力部１３５、第二受信部１３６は出力装置１３ａ～１３ｈにおいて共通の構成要素であり、復号化鍵取得部１３２ａ、ノード鍵格納部１３３ａ、第二復号化部１３７ａ、個別鍵格納部１３８ａは、出力装置１３ａ固有の構成要素である。

【００６６】

（１）第一受信部１３１

第一受信部１３１が、サーバ１２から暗号化コンテンツＥＮＣＣＮＴ及び暗号化コンテ

ンツ鍵群ＥＮＣＣＤＫＧを受信した場合、受信した暗号化コンテンツ鍵群ＥＮＣＣＤＫＧを復号化鍵取得部１３２ａに出力し、その後、暗号化コンテンツＥＮＣＣＮＴを第一復号化部１３４に出力する。

【００６７】

（２）復号化鍵生成部１３２ａ

復号化鍵生成部１３２ａが、第一受信部１３１から暗号化コンテンツ鍵群ＥＮＣＣＤＫＧを受信した場合、まず、図１９で示すようなノード鍵格納部１３３ａにアクセスし、割当ノード復号化鍵群ＡＮＤＫＧａを取得する。そして、割当ノード復号化鍵群ＡＮＤＫＧａを構成している４つのノード復号化鍵を取得する。例えば、図５のような割当ノード復号化鍵群ＡＮＤＫＧａの場合、第０ノード復号化鍵ＮＤＫ０と第１ノード復号化鍵ＮＤＫ１と第３ノード復号化鍵ＮＤＫ３と第７ノード復号化鍵ＮＤＫ７を取得することになる。その後、受信した暗号化コンテンツ鍵群ＥＮＣＣＤＫＧの中から、割当ノード復号化鍵群ＡＮＤＫＧａに含まれていた４つのノード復号化鍵のいずれかに対応する暗号文を探索する。例えば、図１４のような暗号化コンテンツ鍵群ＥＮＣＣＤＫＧの場合、暗号化第７ノード復号化鍵ＥＮＣＮＤＫ７＝Ｅｎｃ（ＮＤＫ７，ＣＤＫ）となる。そして、割当ノード復号化鍵群ＡＮＤＫＧａに含まれていた４つのいずれかのノード復号化鍵を用いて、対応する暗号化ノード復号化鍵を復号化することによって、コンテンツ復号化鍵ＣＤＫを取得する。その後、コンテンツ復号化鍵ＣＤＫを第一復号化部１３４へ出力する。

【００６８】

（３）ノード鍵格納部１３３ａ

ノード鍵格納部１３３ａは、図１９で示すように、割当ノード復号化鍵群ＡＮＤＫＧａを保持するものである。このノード鍵格納部１３３ａへは、復号化鍵生成部１３２ａ及び第二復号化部１３７ａからアクセス可能である。

（４）第一復号化部１３４

第一復号化部１３４は、第一受信部１３１から暗号化コンテンツＥＮＣＣＮＴを受信し、復号化鍵取得部１３２ａからコンテンツ復号化鍵ＣＤＫを受信した場合、そのコンテンツ復号化鍵ＣＤＫに基づいて暗号化コンテンツＥＮＣＣＮＴの復号化を行う。ここで復号化に使用するアルゴリズムは、例えば、ブロック暗号のＡＥＳ方式やＤＥＳ方式などであり、サーバ１２の暗号化部１２２で用いるアルゴリズムと同じ方式を用いる。復号化した復号化コンテンツＤＥＣＣＮＴ＝Ｄｅｃ（ＣＤＫ，ＥＮＣＣＮＴ）を出力部１３５へ出力する。ここで、Ｄｅｃ（Ｋ，Ｃ）は復号化鍵Ｋをもとに、暗号文Ｃを復号化した際の復号文とする。

【００６９】

（５）出力部１３５

出力部１３５は、第一復号化部１３４から復号化コンテンツＤＥＣＣＮＴを受信した場合、受信した復号化コンテンツＤＥＣＣＮＴを外部へ出力する。

（６）第二受信部１３６

第二受信部１３６が、サーバ１２から鍵更新情報ＵＰＤＫＥＹを受信した場合、受信した鍵更新情報ＵＰＤＫＥＹを第二復号化部１３７ａに出力する。

【００７０】

（７）第二復号化部１３７ａ

第二復号化部１３７ａは、第二受信部１３６から鍵更新情報ＵＰＤＫＥＹを受信した場合、まず図２０に示すような個別鍵格納部１３８ａから出力装置識別子ＡＩＤａ及び個別鍵ＩＫａを取得する。そして、受信した鍵更新情報ＵＰＤＫＥＹの中から、個別鍵格納部１３８ａに格納されていた出力装置識別子ＡＩＤａに対応する暗号化割当ノード復号化鍵群ＥＮＣＡＮＤＫＧａを探索する。そして、個別鍵格納部１３８ａに格納されていた個別鍵ＩＫａに基づいて、その対応する暗号化割当ノード復号化鍵群ＥＮＣＡＮＤＫＧａの復号化を行い、その復号化した割当ノード復号化鍵群ＡＮＫａをノード鍵格納部１３３ａに格納する。

【００７１】

（８）個別鍵格納部１３８ａ
個別鍵格納部１３８ａは、図２０で示すように、出力装置識別子ＡＩＤａ及び個別鍵ＩＫａを保持するものである。この個別鍵格納部１３８ａへは、第二復号化部１３７ａからアクセス可能である。
＜出力装置１３ａの動作＞
以上で、出力装置１３ａの構成について説明を行ったが、ここで出力装置１３ａの動作について説明する。まず、暗号化されたコンテンツＥＮＣＣＮＴを受信時した場合の動作について図２１に示すフローチャートを用いて説明する。そして、鍵更新情報ＵＰＤＫＥＹを受信した際の動作について図２２に示すフローチャートを用いて説明する。
【００７２】
≪暗号化コンテンツ受信時の動作≫
第一受信部１３１が、暗号化コンテンツＥＮＣＣＮＴ及び暗号化コンテンツ鍵群ＥＮＣＣＤＫＧを受け取った場合、ステップＳ１３０２に進む。受信していない場合、終了する（Ｓ１３０１）。
第一受信部１３１は、受信した暗号化コンテンツ鍵群ＥＮＣＣＤＫＧを復号化鍵取得部１３２ａに出力する（Ｓ１３０２）。
【００７３】
暗号化コンテンツ鍵群ＥＮＣＣＤＫＧを受信した復号化鍵取得部１３２ａは、ノード鍵格納部１３３ａにアクセスして、割当ノード復号化鍵群ＡＮＤＫＧａを取得する（Ｓ１３０３）。
復号化鍵取得部１３２ａは、割当ノード復号化鍵群ＡＮＤＫＧａから４つのノード復号化鍵を取得する。そして、暗号化コンテンツ鍵群ＥＮＣＣＤＫＧの中において、その４つのノード復号化鍵のいずれかに対応づけられている暗号化ノード復号化鍵を探索し、その暗号化ノード復号化鍵を対応する４つのいずれかのノード復号化鍵を用いて復号化することによって、コンテンツ復号化鍵ＣＤＫを取得する（Ｓ１３０４）。
【００７４】
復号化鍵生成部１３２ａは、コンテンツ復号化鍵ＣＤＫを第一復号化部１３４へ出力する（Ｓ１３０５）。
第一復号化部１３４は、受信したコンテンツ復号化鍵ＣＤＫを基に、暗号化コンテンツＥＮＣＣＮＴの復号化を行い、復号化コンテンツＤＥＣＣＮＴを取得する（Ｓ１３０６）。
【００７５】
第一復号化部１３４は、復号化コンテンツＤＥＣＣＮＴを、出力部１３５へ出力する（Ｓ１３０７）。
出力部１３５は、第一復号化部１３４から復号化コンテンツＤＥＣＣＮＴを受信し、受信した復号化コンテンツＤＥＣＣＮＴを外部へ出力する。終了する（Ｓ１３０８）。
≪鍵更新情報ＵＰＤＫＥＹの受信時の動作≫
第二受信部１３６が鍵更新情報ＵＰＤＫＥＹを受信した場合、ステップＳ１３５２に進む。受信していない場合、終了する（Ｓ１３５１）。
【００７６】
第二受信部１３６は、受信した鍵更新情報ＵＰＤＫＥＹを第二復号化部１３７ａに出力する（Ｓ１３５２）。
第二復号化部１３７ａは、個別鍵格納部１３８ａから出力装置識別子ＡＩＤａ及び個別鍵ＩＫａを取得する（Ｓ１３５３）。
第二復号化部１３７ａは、受信した鍵更新情報ＵＰＤＫＥＹの中から、出力装置識別子ＡＩＤａに対応する暗号化割当ノード復号化鍵群ＥＮＣＡＮＤＫＧａを取得する（Ｓ１３５４）。
【００７７】
第二復号化部１３７ａは、個別鍵ＩＫａに基づいて、暗号化割当ノード復号化鍵群ＥＮＣＡＮＤＫＧａの復号化を行い、割当ノード復号化鍵群ＡＮＤＫＧａを取得する（Ｓ１３

５５）。
第二復号化部１３７ａは、割当ノード復号化鍵群ＡＮＤＫＧａをノード鍵格納部１３３ａに格納し、終了する（Ｓ１３５６）。
【００７８】
以上が、コンテンツ配信システム１の構成要素である出力装置１３ａの構成と動作である。なお、出力装置１３ａと他のいずれの出力装置１３ｂ～１３ｈとで異なる部分については、ノード鍵格納部１３３ａにおいて出力装置１３ａ～１３ｈ毎に異なる割当ノード復号化鍵群ＡＮＫａ～ＡＮＫｈが格納されている点と、個別鍵格納部１３８ａにおいて出力装置１３ａ～１３ｈ毎に異なる出力装置識別子ＡＩＤａ～ｎ及び個別鍵ＩＫａ～ＩＫｈが格納されている点と、復号化鍵取得生成部１３２ａにおいて出力装置１３ａ～１３ｈ毎に異なる割当ノード復号化鍵群ＡＮＫａ～ＡＮＫｈを用いる点と、第二復号化部１３７ａにおいて出力装置１３ａ～１３ｈ毎に異なる個別鍵ＩＫａ～ＩＫｈを用いる点が異なる。
【００７９】
＜実施の形態１の動作検証＞
本実施の形態１において、それぞれの出力装置１３ａ～１３ｈには各々異なる割当ノード復号化鍵群ＡＮＤＫＧａ～ＡＮＤＫＧｈが割り当てられているにもかかわらず、全出力装置１３ａ～１３ｈにおいて同じコンテンツ復号化鍵ＣＤＫが導出出来る理由について説明する。サーバ１２は、ノード暗号化鍵群の中から各出力装置１３ａ～１３ｈが必ず保持しているノード復号化鍵から成る複数のノード復号化鍵に対応するノード暗号化鍵を選択して、その複数のノード暗号化鍵群を基にコンテンツ復号化鍵ＣＤＫを暗号化している。そのため、出力装置１３ａ～１３ｈでは同じコンテンツ復号化鍵ＣＤＫが導出出来る。
【００８０】
実際に運用する場合には、例えば、図２８から図３３で示すようなコンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵を、周期的に変更する。そうすることによって、出力装置では必ず末端（第３階層）のノード復号化鍵を使用しないと、周期のある一定期間ではコンテンツ復号化鍵を得られないように出来る。また、もし末端のノード復号化鍵を埋め込んだ不正な出力装置が出回ったとしても、その末端のノード復号化鍵を調査することで、どの出力装置の個別鍵が漏洩したのか特定することが出来る。
【００８１】
＜実施の形態１の効果＞
本発明の実施の形態１によって、コンテンツ復号化鍵を埋め込んだ不正な出力装置を無効化するために、鍵発行センタがコンテンツ暗号化鍵及び対応するコンテンツ復号化鍵のペアを更新したときに、出力装置へ配信するデータサイズを削減できるようになった。具体的には、例えば、８台の出力装置を想定する場合、従来例においてコンテンツ暗号化鍵ＣＥＫ及び対応するコンテンツ復号化鍵ＣＤＫのペアを更新するには、コンテンツ復号化鍵をそれぞれの個別鍵を用いて暗号化した際の暗号文として計８個が必要であった。しかし、本実施の形態においてコンテンツ暗号化鍵ＣＥＫ及び対応するコンテンツ復号化鍵ＣＤＫのペアを更新するには、例えば、図２８から図３２のような複数のノード暗号化鍵の割り当てを考えた場合、コンテンツ復号化鍵をそれぞれ４つのノード暗号化鍵を用いて暗号化した際の暗号文として計４個となり、データサイズの削減が実現出来る。このことによって、本実施の形態では、コンテンツ暗号化鍵及び対応するコンテンツ復号化鍵のペアをより多くの回数更新することが出来るようになるため、漏洩元の追跡が不可能なコンテンツ復号化鍵を埋め込んだ不正な出力装置を作成する攻撃に対する耐性を増すことが出来た。
【００８２】
＜変形例＞
上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において主な態様で実施し得るものである。以下のような場合も本発明に含まれる。
（１）通信路１０は、地上波又は衛星等の放送網であっても良い。

【００８３】
（２）出力装置１３ａ～１３ｈの数は８台でなくても良い。これは、鍵の割り当てを決める木構造の深さを変更する等によって容易に実現可能である。
（３）本実施の形態では、各末端ノードに一台の出力装置を設定していたが、一つの末端に複数の出力装置を設定しても良い。
（４）ノード暗号化鍵及び対応するノード復号化鍵が同一の値であっても良い。これにより、鍵情報格納部１２３は、ノード暗号化鍵群及びノード復号化鍵群のどちらかを格納するだけで十分となる。これは、コンテンツ鍵選択部１２４及び復号化鍵取得部１３２ａにおいて共通鍵暗号などを用いれば実現可能である。
【００８４】
（５）コンテンツ暗号化鍵ＣＥＫ及び対応するコンテンツ復号化鍵ＣＤＫが同一の値であっても良い。これにより、鍵情報格納部１２３は、コンテンツ暗号化鍵及びコンテンツ復号化鍵のどちらかを格納するだけで十分となる。これは、暗号化部１２２及び復号化部１３４において共通鍵暗号などを用いれば実現可能である。
（６）鍵の割り当てを決める木構造は、図２のような形に限定されるものではない。例えば、図２３で示すように２つの木構造を利用していても良いし、図２４で示すように４つの木構造を利用しても良いし、それ以上の数の木構造を利用していても良い。また、図２５のように、図２の木構造から第２階層の全てのノードをなくしたようなものでも良く、さらに、図２６のように、図２の木構造から第１階層と第２階層の全てのノードをなくしたものでも良い。
【００８５】
（７）鍵の割り当てを決める木構造に関して、図２では１つのノードが２つの子ノードを持つ２分木であったが、Ｍ分木（Ｍは３以上の自然数）でも良い。例えば、図２７で示すような３分木であっても良い。さらに、階層毎に、分木数が異なっていても良い。
（８）出力装置の無効化を行う機能を、鍵発行センタ１１ではなくサーバ１２が持つようにしても良い。つまり、サーバ１２が出力装置識別子ＡＩＤａ～ＡＩＤｈのいずれかを受信し、その出力装置識別子ＡＩＤａ～ＡＩＤｈのいずれかを基に、鍵更新情報ＵＰＤＫＥＹを複数の出力装置１３ａ～１３ｈに配信するようにしても良い。
【００８６】
（９）鍵発行センタ１１のノード鍵生成部１１１は、外部からノード鍵生成要求情報ＲＥＱ１を受信するようにして、そのノード鍵生成要求情報ＲＥＱ１に基づき、複数のノード暗号化鍵及び対応するノード復号化鍵のペアを生成するようにしても良い。
（１０）サーバ１２のコンテンツ鍵生成部１２７は、外部からコンテンツ鍵生成要求情報ＲＥＱ３を受信するようにして、そのコンテンツ鍵生成要求情報ＲＥＱ３に基づき、コンテンツ暗号化鍵ＣＥＫ及び対応するコンテンツ復号化鍵ＣＤＫのペアを生成するようにしても良い。
【００８７】
（１１）サーバ１２の送信部１２５は、前回送信した暗号化コンテンツ鍵群ＥＮＣＣＤＫＧから変更がない場合は、暗号化コンテンツＥＮＣＣＮＴだけを出力装置１３ａ～１３ｈに送信するようにして、暗号化コンテンツＥＮＣＣＮＴだけを受信した出力装置１３ａ～１３ｈは、前回生成したコンテンツ復号化鍵ＣＤＫを基に、暗号化コンテンツＥＮＣＣＮＴを復号化するようにしても良い。
【００８８】
（１２）コンテンツ復号化鍵を暗号化する際に用いる複数のノード暗号化鍵の選択方法に関して、各出力装置１３ａ～１３ｈが必ず１つずつ持つノード復号化鍵に対応するノード暗号化鍵を選択しなくてもよい。例えば、いくつかの出力装置が２つ以上持っているノード復号化鍵に対応するノード暗号化鍵を選択しても良いし、いくつかの出力装置が１つも持っていないノード復号化鍵に対応するノード暗号化鍵を選択しても良い。
【００８９】
（１３）コンテンツ復号化鍵ＣＤＫを暗号化するのに用いるノード暗号化鍵群をパター

ン化して、サーバ１２及び出力装置１３ａ～１３ｈで共有するようにしても良い。例えば、図２８のようなノード暗号化鍵群パターンを第１パターンＰ１、図２９のようなノード暗号化鍵群パターンを第２パターンＰ２、図３０のようなノード暗号化鍵群パターンを第３パターンＰ３、図３１のようなノード暗号化鍵群パターンを第４パターンＰ４とし、また、暗号化コンテンツ鍵群ＥＮＣＣＤＫＧの中に第１パターンＰ１から第４パターンＰ４のいずれかを含むようにして、また、各出力装置１３ａ～１３ｈには、各ノード暗号化鍵群パターンとノード復号化鍵に関する対応情報を保持しており、復号化鍵取得部１３２ａはその対応情報を基に、コンテンツ復号化鍵ＣＤＫを取得するようにしても良い。

【００９０】

（１４）末端ノードを除く各々のノードに対して、複数のノード暗号化鍵及び対応するノード復号化鍵を設定しても良い。

【産業上の利用可能性】

【００９１】

本発明にかかるコンテンツ配信システムは、出力装置に埋め込まれている鍵が漏洩し、その鍵を用いて不正な出力装置が作成されたとしても、コンテンツ提供者はその不正な出力装置に埋め込まれている鍵情報を調査することによってその漏洩元を追跡出来るという効果を有し、インターネット等の通信路を用いてコンテンツを配信する際に有用である。また放送等の用途にも応用できる。

【図面の簡単な説明】

【００９２】

【図１】本発明の実施の形態１におけるコンテンツ配信システム１の概要図

【図２】出力装置１３ａ～１３ｈに対するノード暗号化鍵及びノード復号化鍵の設定方法の一例

【図３】本発明の実施の形態１におけるノード暗号化鍵群ＡＬＬＮＥＫの一例を示す図

【図４】本発明の実施の形態１における鍵発行センタ１１の構成例を示す図

【図５】本発明の実施の形態１における割当ノード復号化鍵群ＡＮＫａの一例を示す図

【図６】本発明の実施の形態１における出力装置対応情報格納部１１３の構成例を示す図

【図７】本発明の実施の形態１における鍵更新情報ＵＰＤＫＥＹの一例を示す図

【図８】本発明の実施の形態１における出力装置１３ａを無効化した後の出力装置対応情報格納部１１３の構成例を示す図

【図９】本発明の実施の形態１における鍵発行センタ１１のノード暗号化鍵、ノード復号化鍵配信時の処理の流れ図

【図１０】本発明の実施の形態１における鍵発行センタ１１の出力装置１３ａ無効化時の処理の流れ図

【図１１】本発明の実施の形態１におけるサーバ１２の構成例を示す図

【図１２】本発明の実施の形態１における鍵情報格納部１２３の構成例を示す図

【図１３】本発明の実施の形態１におけるノード復号化鍵群ＡＬＬＮＤＫの構成例を示す図

【図１４】本発明の実施の形態１における暗号化コンテンツ鍵群ＥＮＣＣＤＫＧの一例を示す図

【図１５】本発明の実施の形態１におけるサーバ１２のコンテンツ配信時の処理の流れ図

【図１６】本発明の実施の形態１におけるサーバ１２のノード暗号化鍵群受信時の処理の流れ図

【図１７】本発明の実施の形態１におけるサーバ１２のコンテンツ鍵更新時の処理の流れ図

【図１８】本発明の実施の形態１における出力装置１３ａの構成例を示す図

【図１９】本発明の実施の形態１におけるノード鍵格納部１３３ａの構成例を示す図
【図２０】本発明の実施の形態１における個別鍵格納部１３８ａの構成例を示す図
【図２１】本発明の実施の形態１におけるサーバ１２の暗号化コンテンツ受信時の処理の流れ図
【図２２】本発明の実施の形態１におけるサーバ１２の鍵更新情報受信時の処理の流れ図
【図２３】出力装置１３ａ～１３ｈに対するノード暗号化鍵及びノード復号化鍵の割り当て方法の別の一例
【図２４】出力装置１３ａ～１３ｈに対するノード暗号化鍵及びノード復号化鍵の割り当て方法の別の一例
【図２５】出力装置１３ａ～１３ｈに対するノード暗号化鍵及びノード復号化鍵の割り当て方法の別の一例
【図２６】出力装置１３ａ～１３ｈに対するノード暗号化鍵及びノード復号化鍵の割り当て方法の別の一例
【図２７】出力装置１３ａ～１３ｉに対するノード暗号化鍵及びノード復号化鍵の割り当て方法の別の一例
【図２８】コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例
【図２９】コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例
【図３０】コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例
【図３１】コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例
【図３２】コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例
【図３３】コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例
【図３４】従来のコンテンツ配信システムの概要図

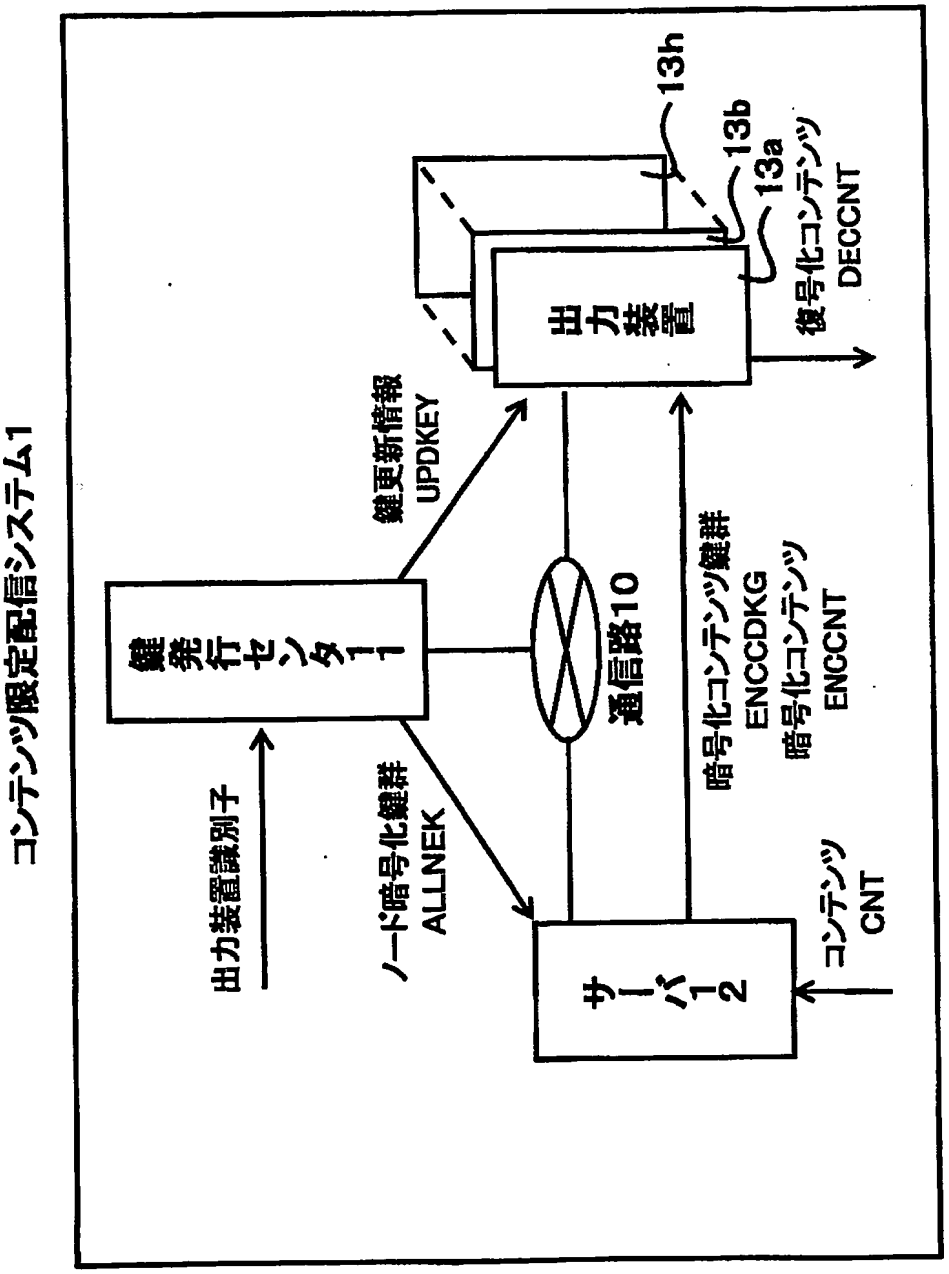
【符号の説明】

【００９３】

１０　通信路
１１　鍵発行センタ
１２　サーバ
１３ａ～１３ｈ　出力装置
１１１　ノード鍵生成部
１１２　第一送信部
１１３　出力装置対応情報格納部
１１４　第一暗号化部
１１５　第二送信部
１１６、１２１　入力部
１１７　対応情報更新部
１２２　暗号化部
１２３　鍵情報格納部
１２４　コンテンツ鍵選択部
１２５　送信部
１２６　受信部
１２７　暗号化コンテンツ鍵生成部
１３１　第一受信部
１３２ａ　復号化鍵取得部

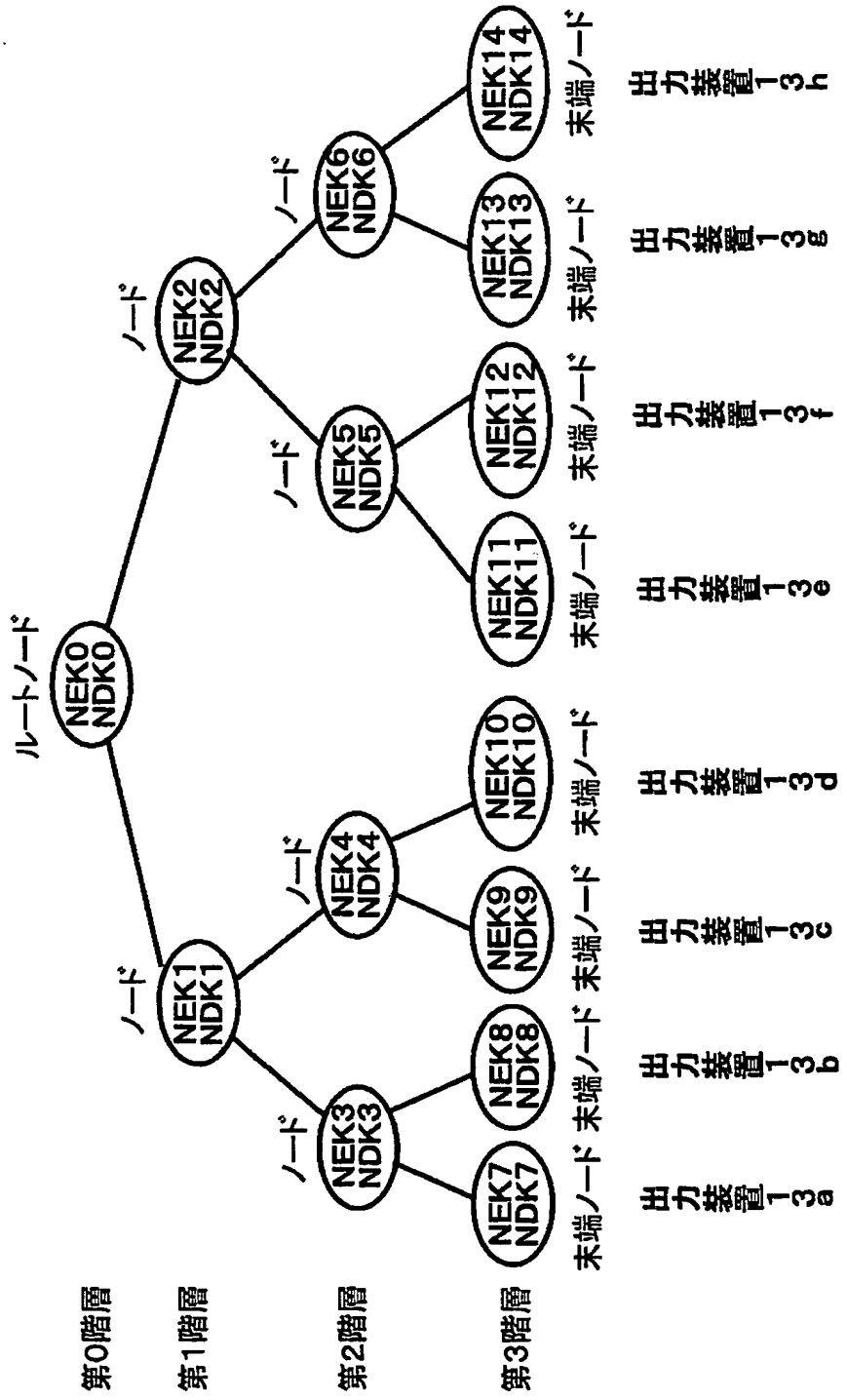
１３３ａ　ノード鍵格納部
１３４　第一復号化部
１３５　出力部
１３６　第二受信部
１３７ａ　第二復号化部
１３８ａ　個別鍵格納部

【書類名】図面
【図１】

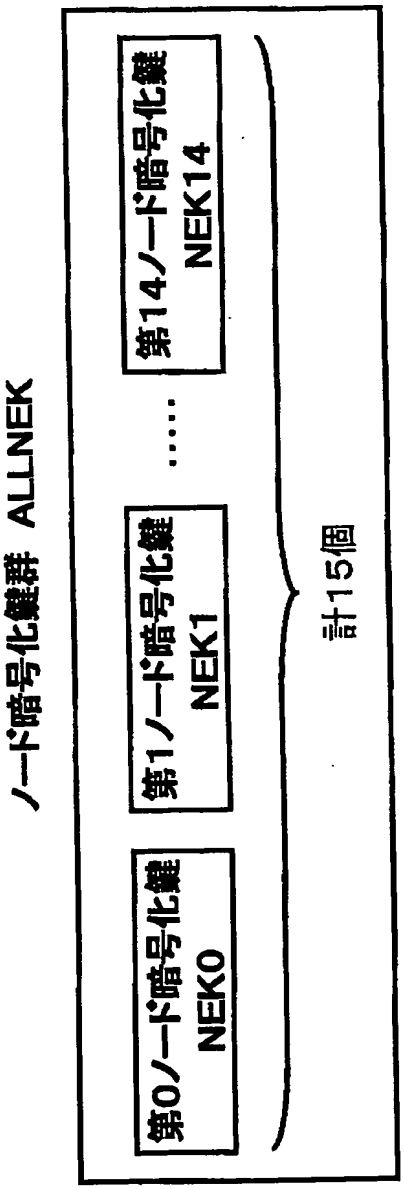

コンテンツ限定配信システム1
鍵発行センタ1
サーバ2
出力装置
通信路10
出力装置識別子
ノード暗号化鍵群
ALLNEK
鍵更新情報
UPDKEY
暗号化コンテンツ鍵群
ENCCDKG
暗号化コンテンツ
ENCCNT
コンテンツ
CNT
復号化コンテンツ
DECCNT
13a
13b
13h

【図２】

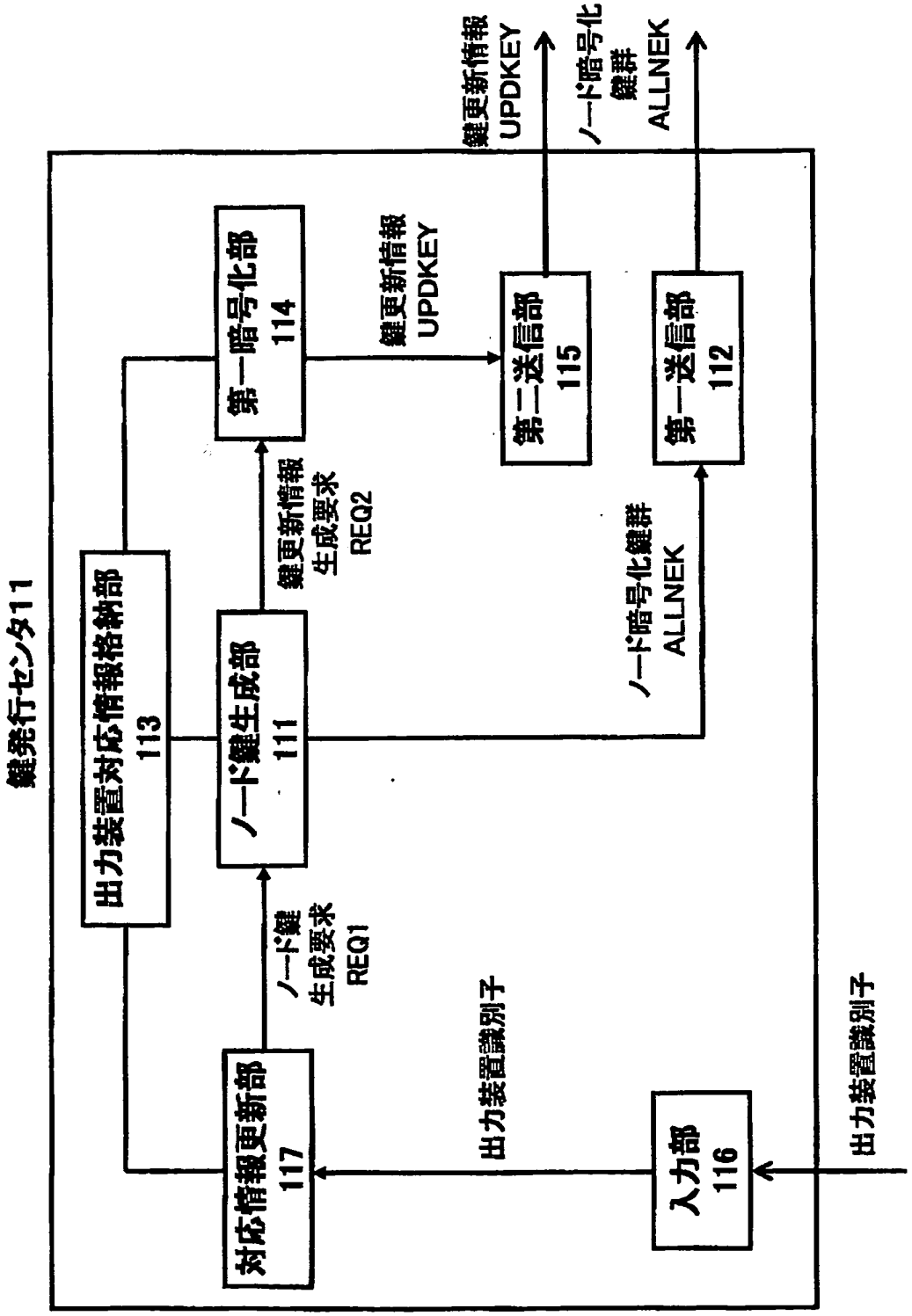
出力装置13a～13hに対するノード暗号化鍵及びノード復号化鍵の設定方法の一例



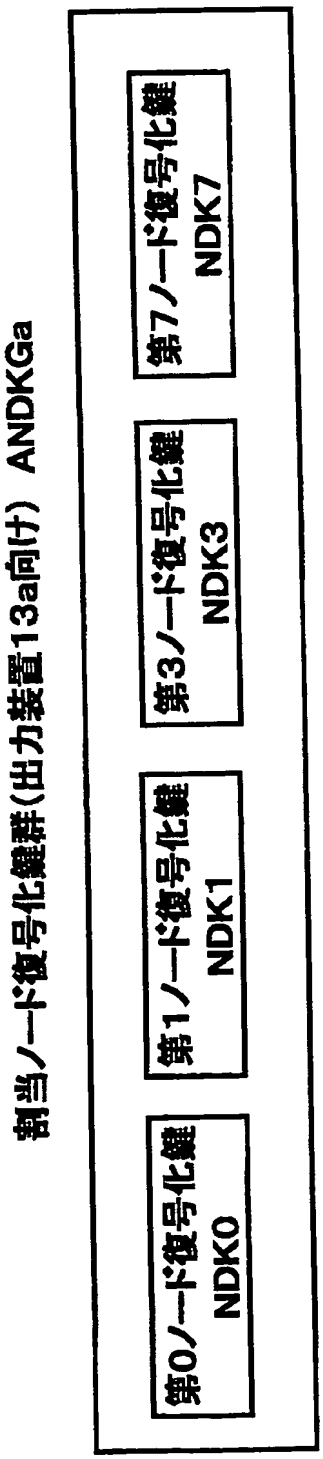
【図３】


ノード暗号化鍵群 ALLNEK
第0ノード暗号化鍵 NEK0
第1ノード暗号化鍵 NEK1
.....
第14ノード暗号化鍵 NEK14
計15個

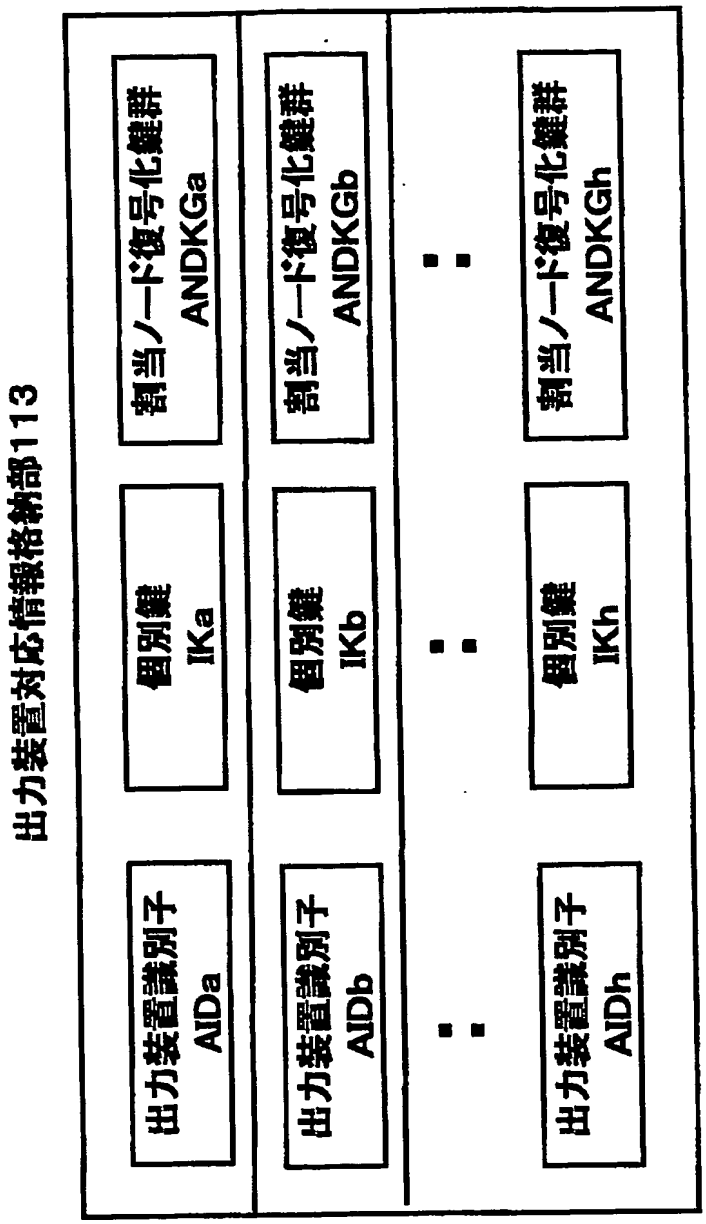
【図４】


鍵発行センタ11
出力装置対応情報格納部 113
ノード鍵生成部 111
対応情報更新部 117
第一暗号化部 114
第二送信部 115
第一送信部 112
入力部 116
鍵更新情報 UPDKEY
ノード暗号化 鍵群 ALLNEK
鍵更新情報 UPDKEY
鍵更新情報 生成要求 REQ2
ノード暗号化鍵群 ALLNEK
ノード鍵 生成要求 REQ1
出力装置識別子
出力装置識別子

【図５】

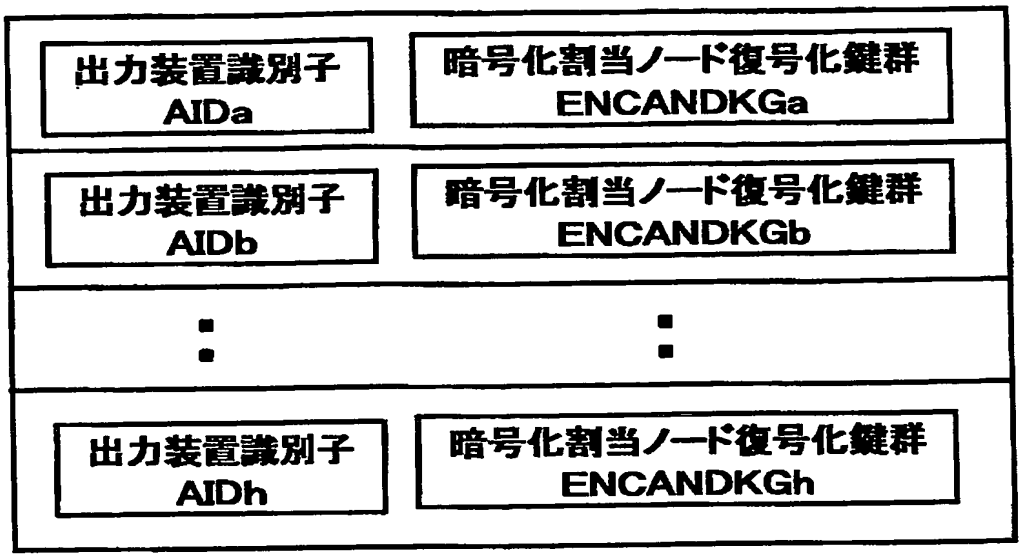

割当ノード復号化鍵群(出力装置13a向け) ANDKGa
第0ノード復号化鍵 NDK0
第1ノード復号化鍵 NDK1
第3ノード復号化鍵 NDK3
第7ノード復号化鍵 NDK7

【図６】

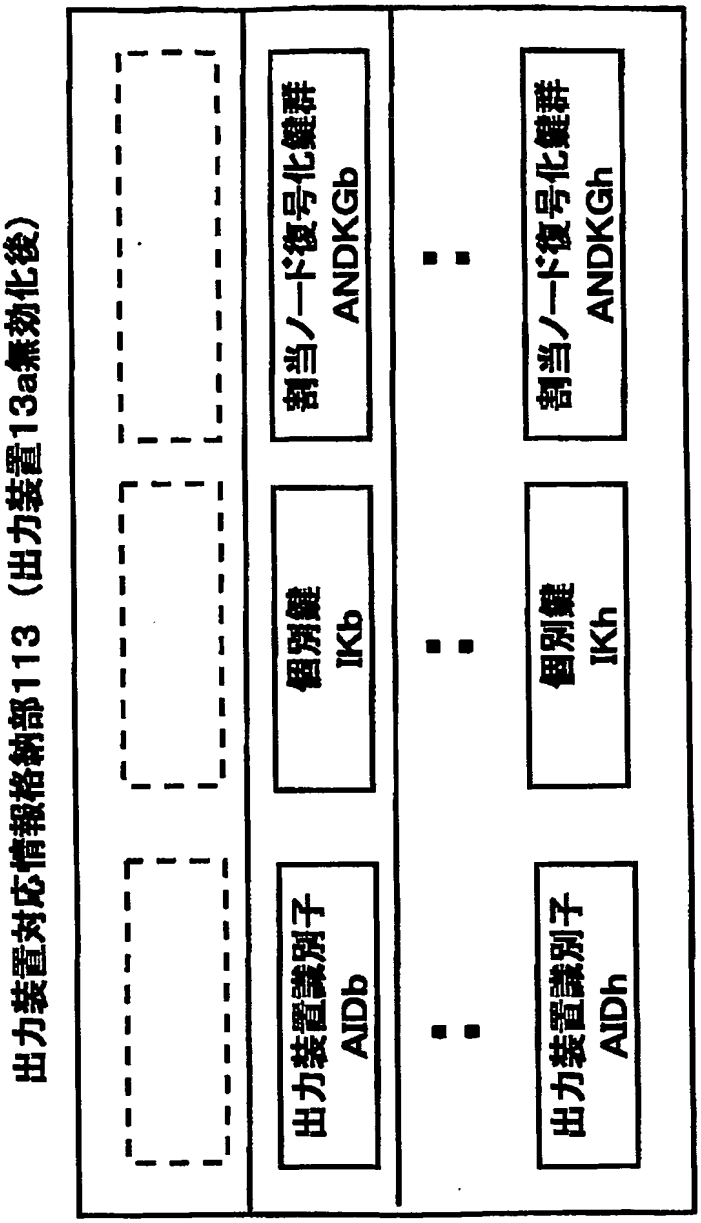

出力装置対応情報格納部113
出力装置識別子
AIDa
個別鍵
IKa
割当ノード復号化鍵群
ANDKGa
出力装置識別子
AIDb
個別鍵
IKb
割当ノード復号化鍵群
ANDKGb
出力装置識別子
AIDh
個別鍵
IKh
割当ノード復号化鍵群
ANDKGh

【図７】

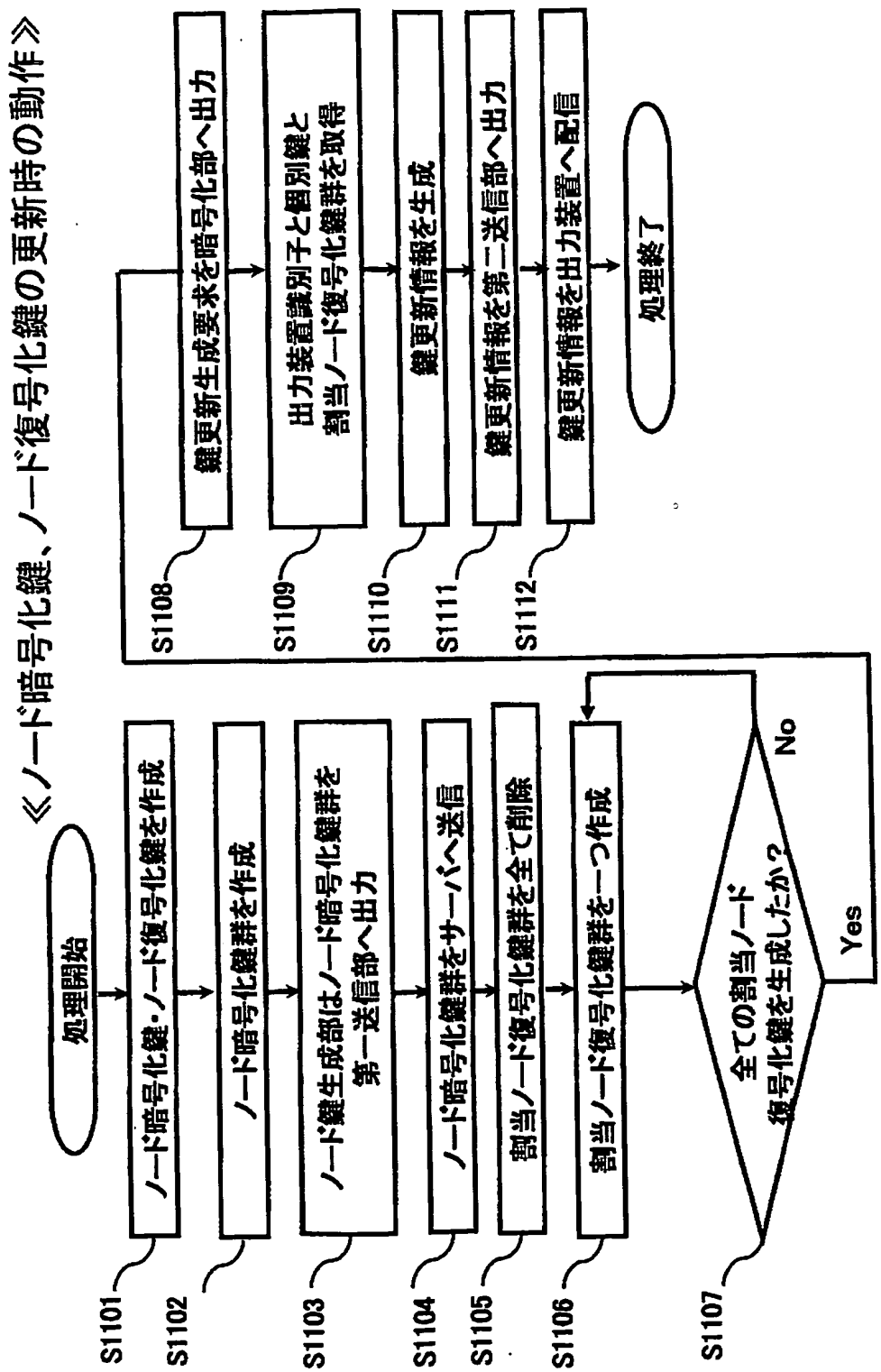
鍵更新情報　UPDKEY



【図８】

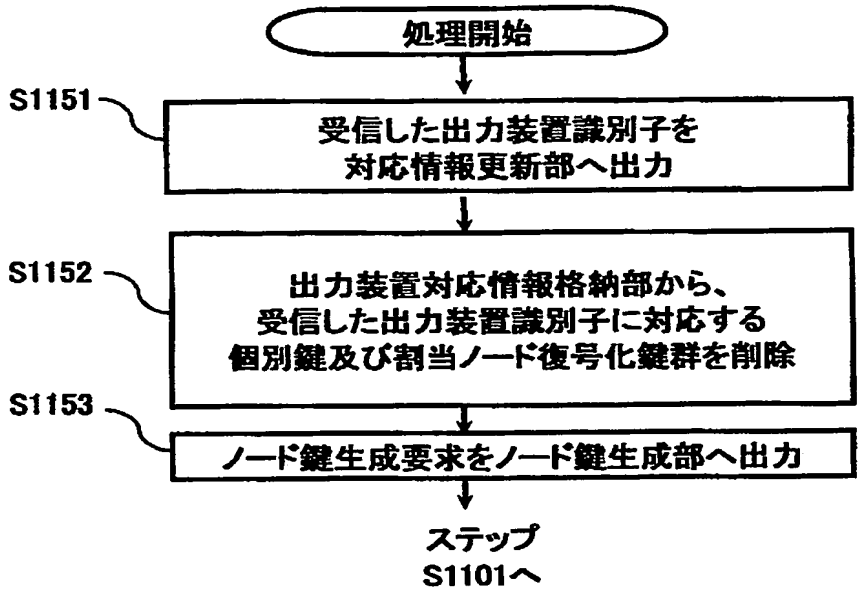

出力装置対応情報格納部113（出力装置13a無効化後）
出力装置識別子
AIDb
個別鍵
IKb
割当ノード復号化鍵群
ANDKGb
出力装置識別子
AIDh
個別鍵
IKh
割当ノード復号化鍵群
ANDKGh

【図９】

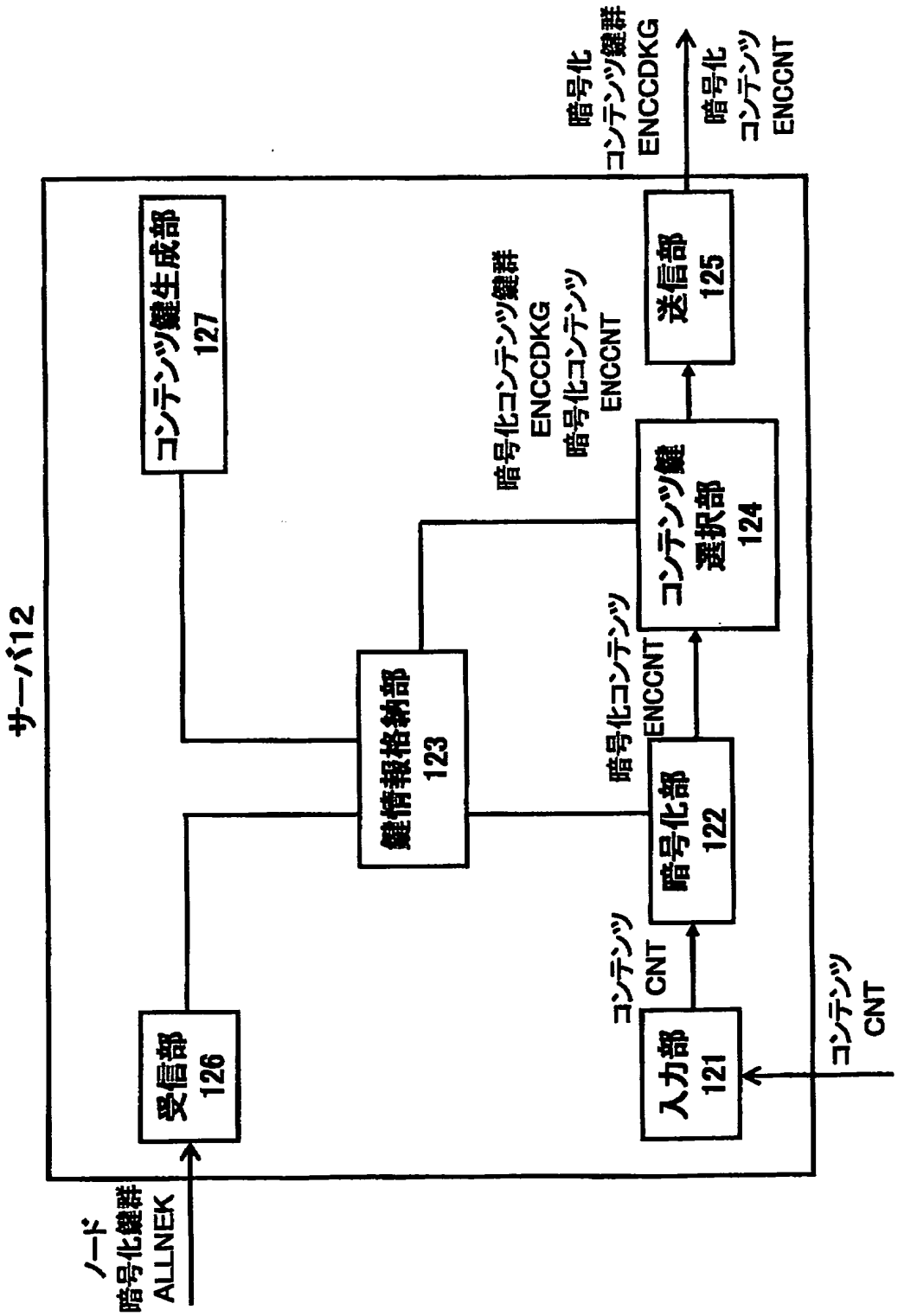

≪ノード暗号化鍵、ノード復号化鍵の更新時の動作≫
処理開始
ノード暗号化鍵・ノード復号化鍵を作成
ノード暗号化鍵群を作成
ノード鍵生成部はノード暗号化鍵群を第一送信部へ出力
ノード暗号化鍵群をサーバへ送信
割当ノード復号化鍵群を全て削除
割当ノード復号化鍵群を一つ作成
全ての割当ノード復号化鍵を生成したか？
No
Yes
鍵更新生成要求を暗号化部へ出力
出力装置識別子と個別鍵と割当ノード復号化鍵群を取得
鍵更新情報を生成
鍵更新情報を第二送信部へ出力
鍵更新情報を出力装置へ配信
処理終了
S1101
S1102
S1103
S1104
S1105
S1106
S1107
S1108
S1109
S1110
S1111
S1112

【図１０】

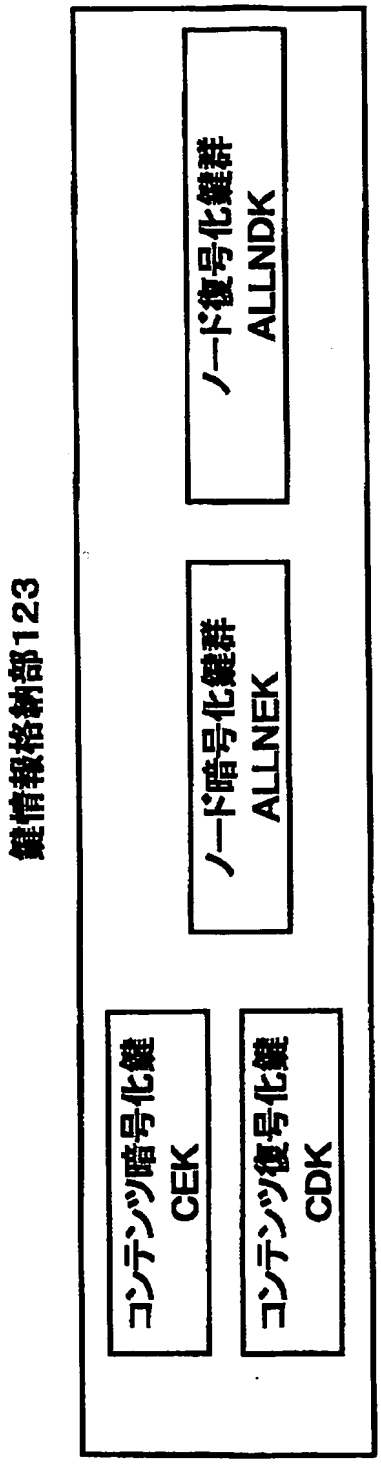
≪出力装置13aを無効化する動作≫



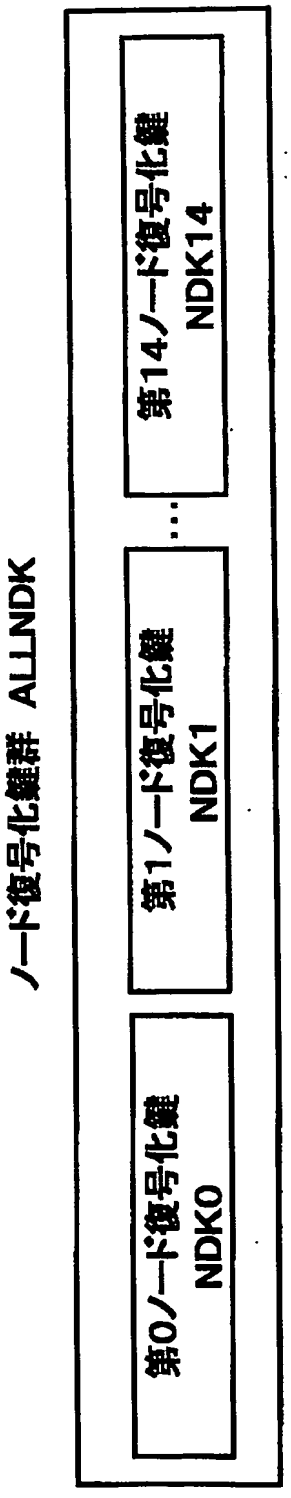
【図１１】


サーバ12
ノード
暗号化鍵群
ALLNEK
受信部
126
入力部
121
コンテンツ
CNT
コンテンツ
CNT
暗号化部
122
暗号化コンテンツ
ENCCNT
鍵情報格納部
123
コンテンツ鍵
選択部
124
暗号化コンテンツ鍵群
ENCCDKG
暗号化コンテンツ
ENCCNT
送信部
125
暗号化
コンテンツ鍵群
ENCCDKG
暗号化
コンテンツ
ENCCNT
コンテンツ鍵生成部
127

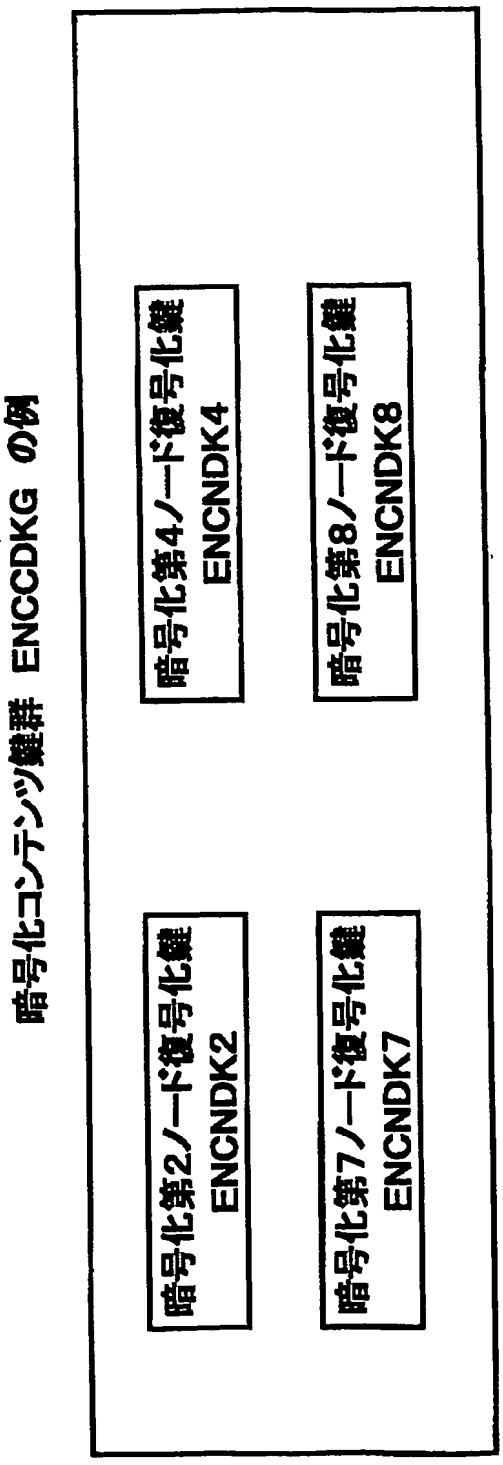
【図１２】


鍵情報格納部123
コンテンツ暗号化鍵
CEK
コンテンツ復号化鍵
CDK
ノード暗号化鍵群
ALLNEK
ノード復号化鍵群
ALLNDK

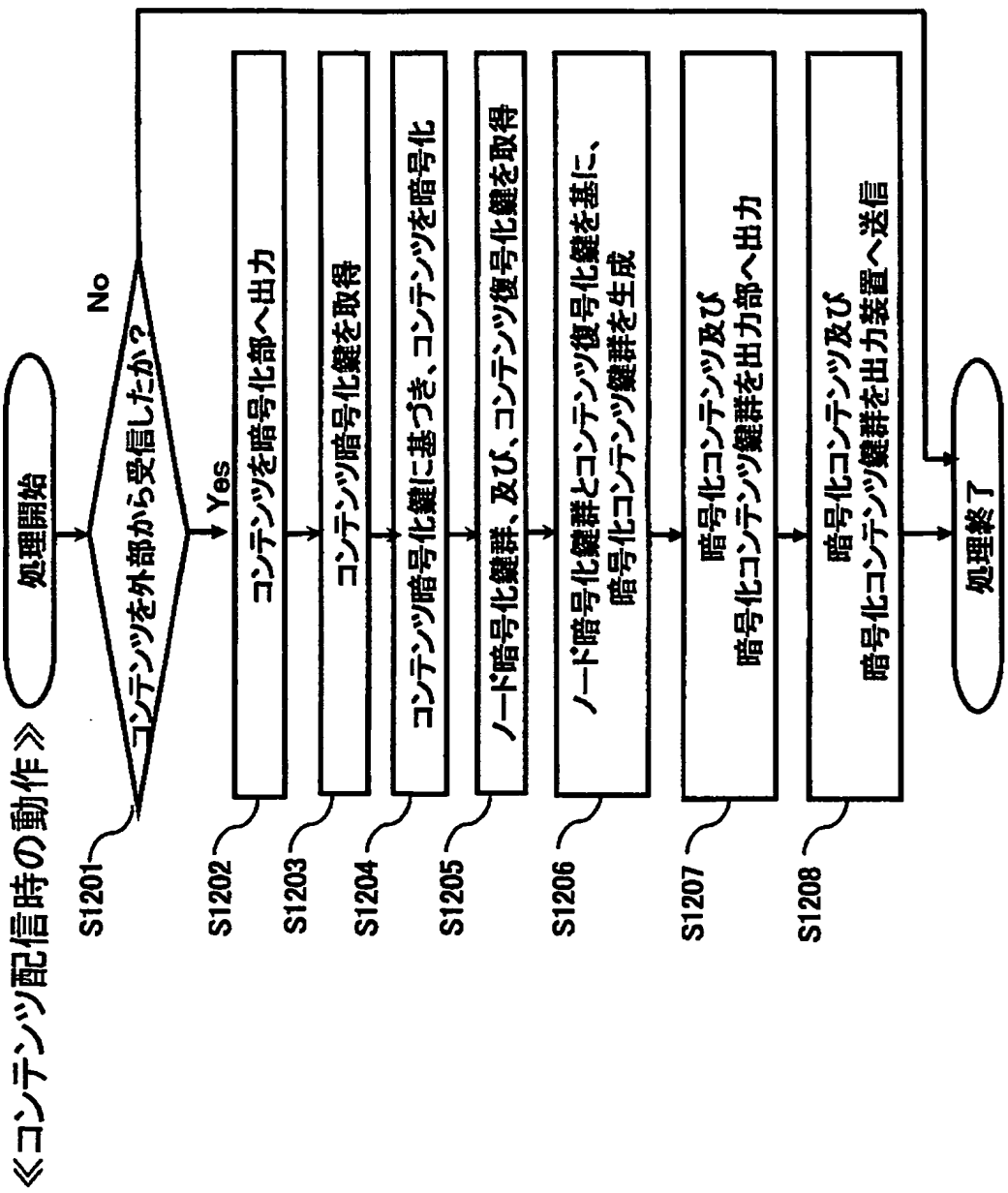
【図１３】


ノード復号化鍵群　ALLNDK
第0ノード復号化鍵
NDK0
第1ノード復号化鍵
NDK1
…
第14ノード復号化鍵
NDK14

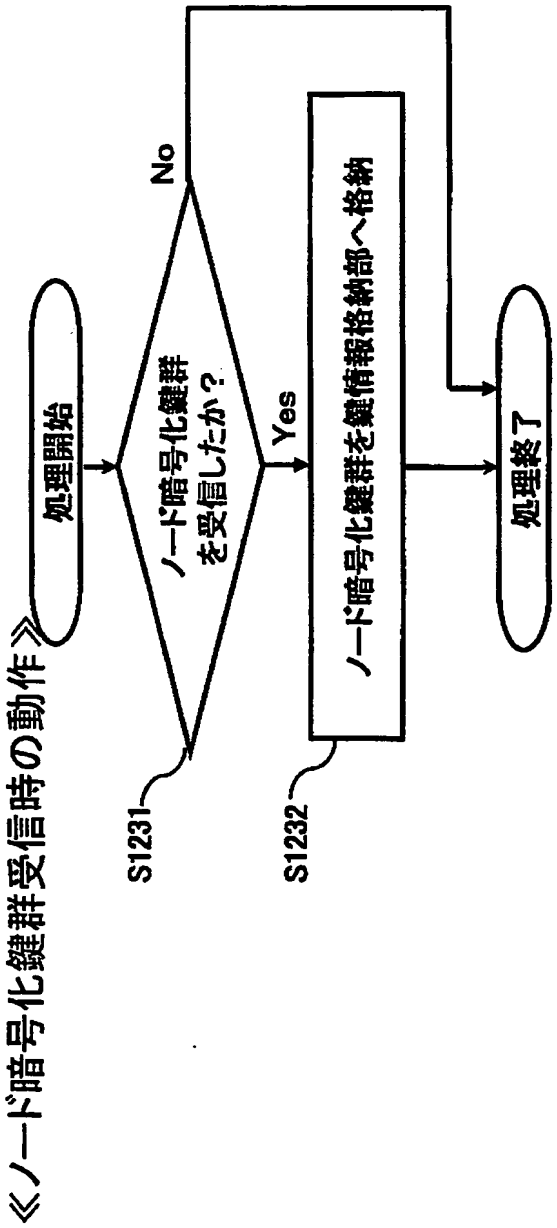
【図１４】


暗号化コンテンツ鍵群　ENCCDKG　の例
暗号化第4ノード復号化鍵
ENCNDK4
暗号化第8ノード復号化鍵
ENCNDK8
暗号化第2ノード復号化鍵
ENCNDK2
暗号化第7ノード復号化鍵
ENCNDK7

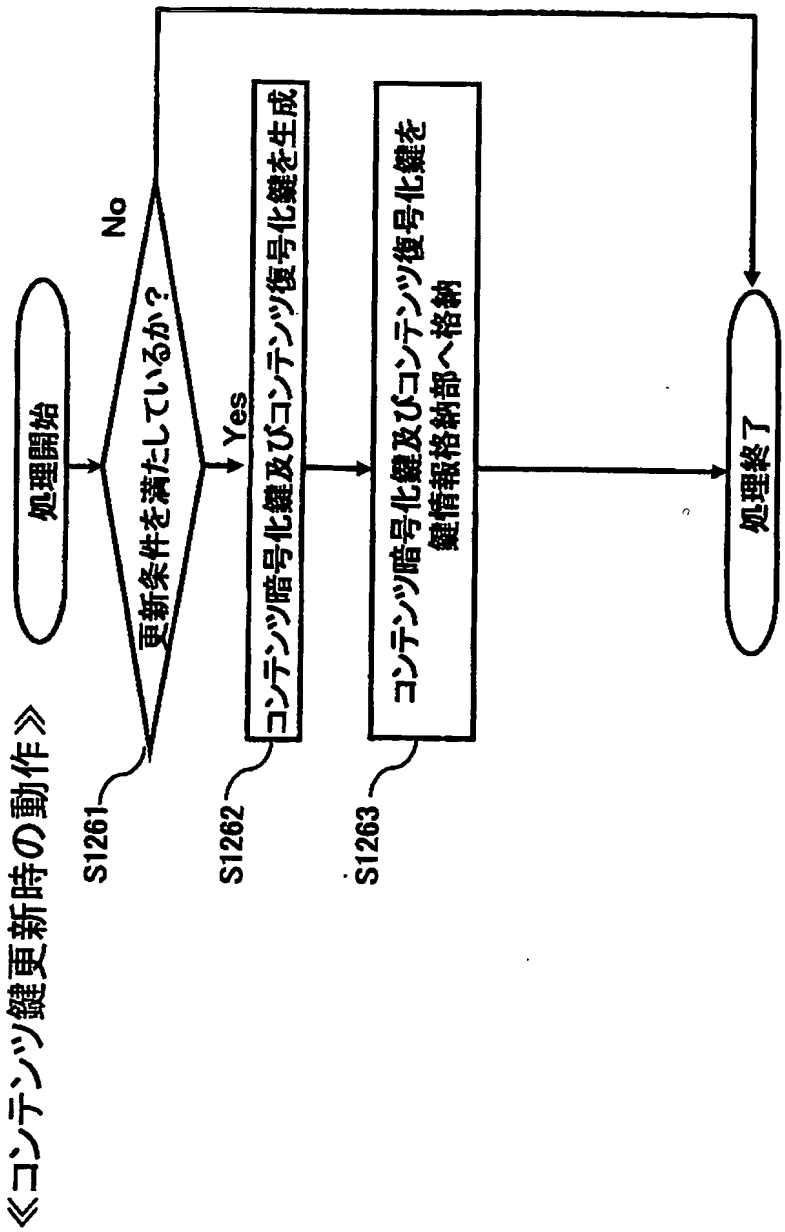
【図１５】


≪コンテンツ配信時の動作≫
処理開始
コンテンツを外部から受信したか？
No
Yes
S1201
コンテンツを暗号化部へ出力
S1202
コンテンツ暗号化鍵を取得
S1203
コンテンツ暗号化鍵に基づき、コンテンツを暗号化
S1204
ノード暗号化鍵群、及び、コンテンツ復号化鍵を取得
S1205
ノード暗号化鍵群とコンテンツ復号化鍵を基に、暗号化コンテンツ鍵群を生成
S1206
暗号化コンテンツ及び暗号化コンテンツ鍵群を出力部へ出力
S1207
暗号化コンテンツ及び暗号化コンテンツ鍵群を出力装置へ送信
S1208
処理終了

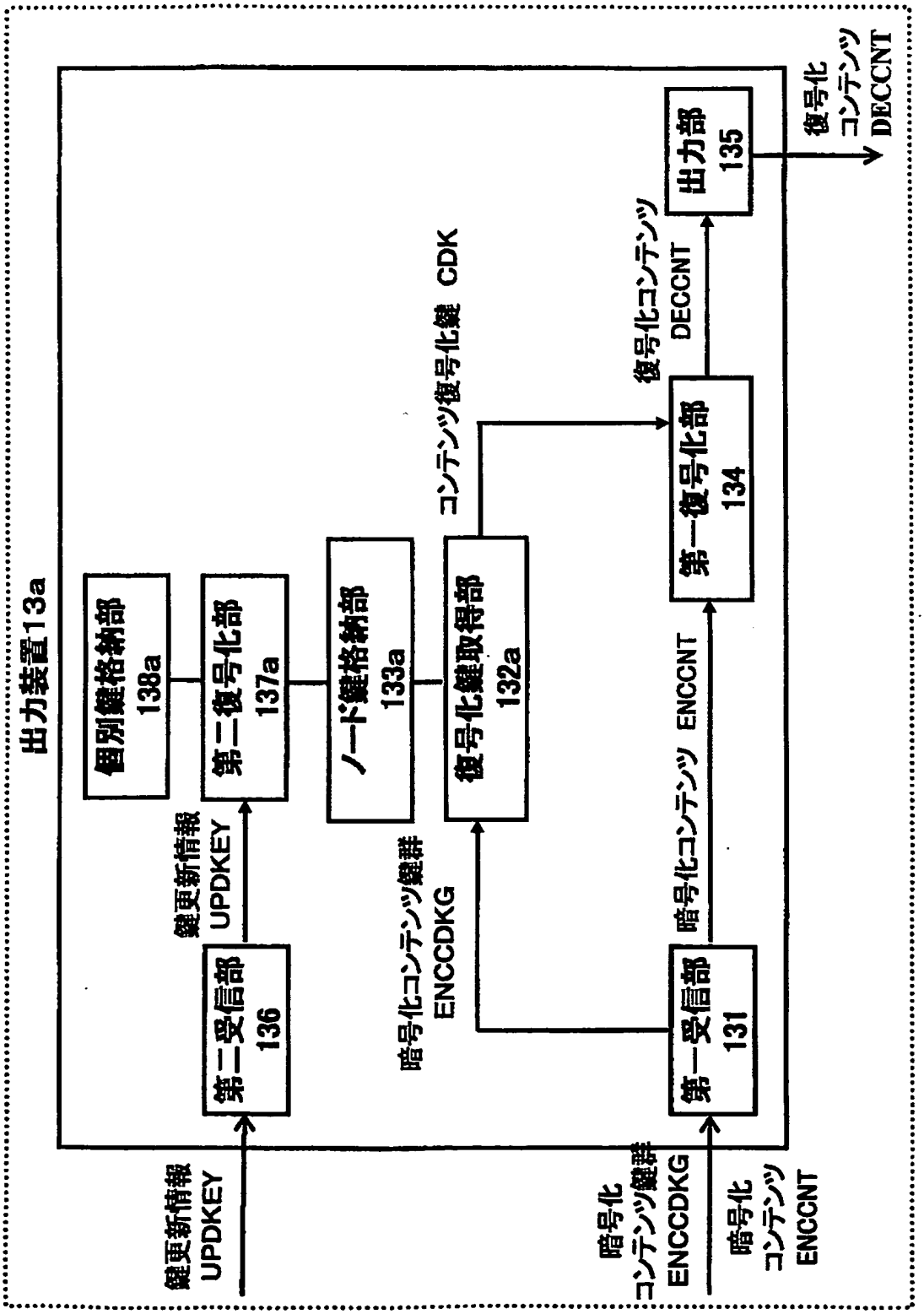
【図１６】


≪ノード暗号化鍵群受信時の動作≫
処理開始
ノード暗号化鍵群を受信したか？
No
Yes
S1231
S1232
ノード暗号化鍵群を鍵情報格納部へ格納
処理終了

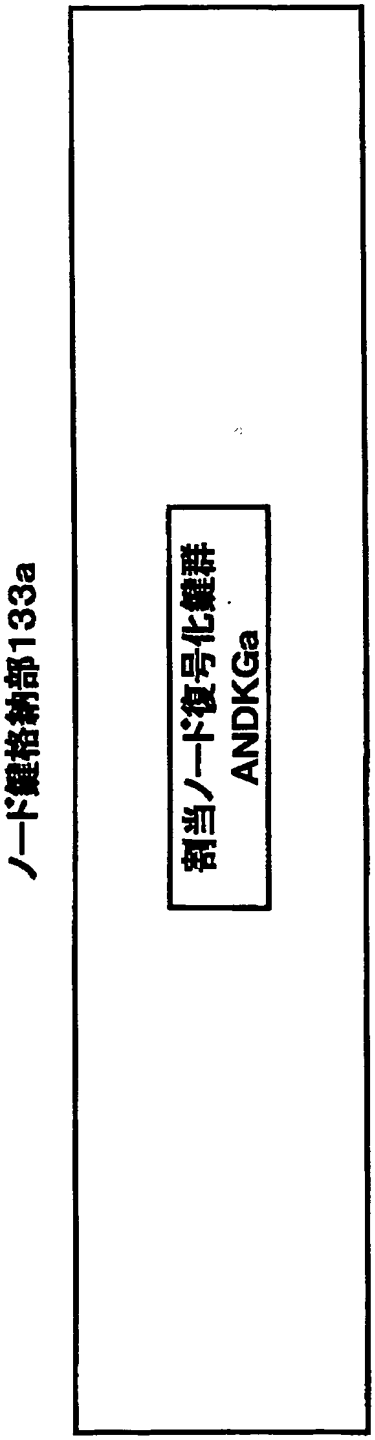
【図１７】


《コンテンツ鍵更新時の動作》
処理開始
更新条件を満たしているか？
No
Yes
S1261
コンテンツ暗号化鍵及びコンテンツ復号化鍵を生成
S1262
コンテンツ暗号化鍵及びコンテンツ復号化鍵を鍵情報格納部へ格納
S1263
処理終了

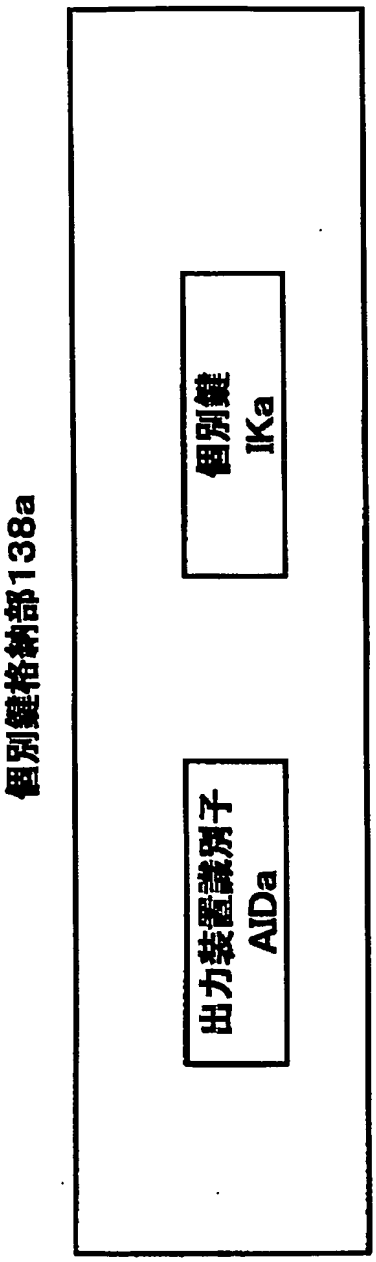
【図１８】


出力装置13a
個別鍵格納部 138a
第二復号化部 137a
ノード鍵格納部 133a
復号化鍵取得部 132a
第一復号化部 134
出力部 135
第二受信部 136
第一受信部 131
鍵更新情報 UPDKEY
暗号化コンテンツ鍵群 ENCCDKG
コンテンツ復号化鍵 CDK
暗号化コンテンツ ENCCNT
復号化コンテンツ DECCNT
復号化コンテンツ DECCNT
鍵更新情報 UPDKEY
暗号化コンテンツ鍵群 ENCCDKG
暗号化コンテンツ ENCCNT
復号化コンテンツ DECCNT

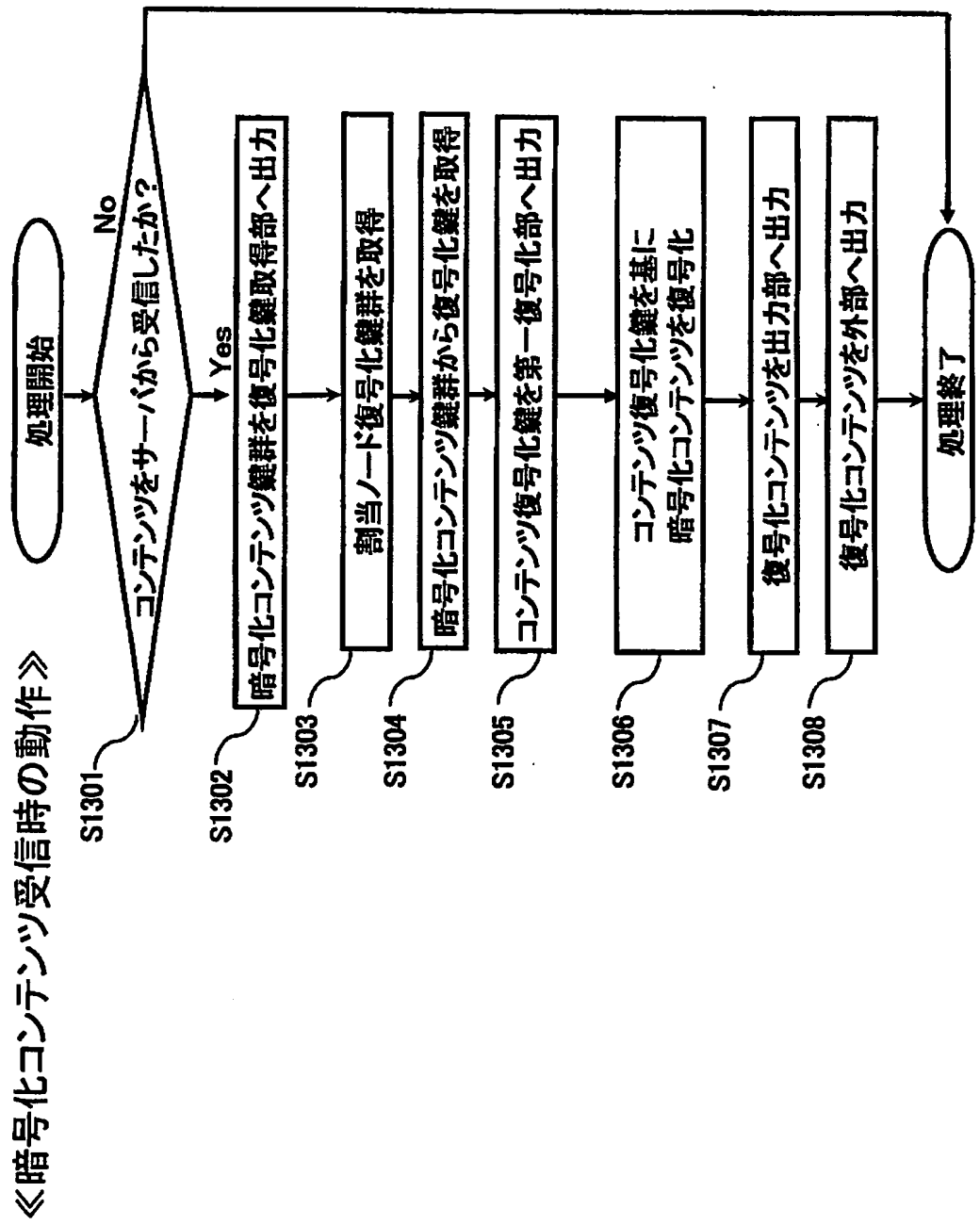
【図１９】



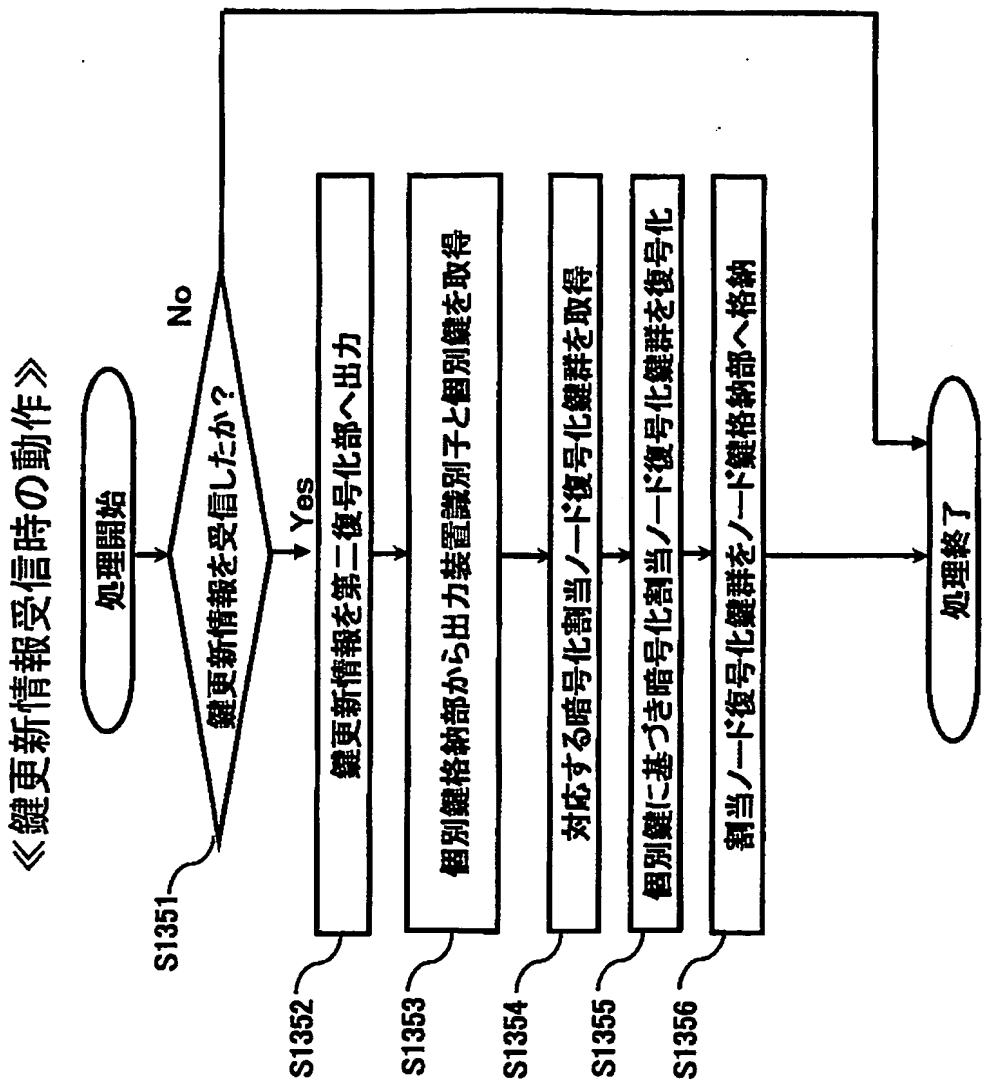
【図２０】



【図２１】

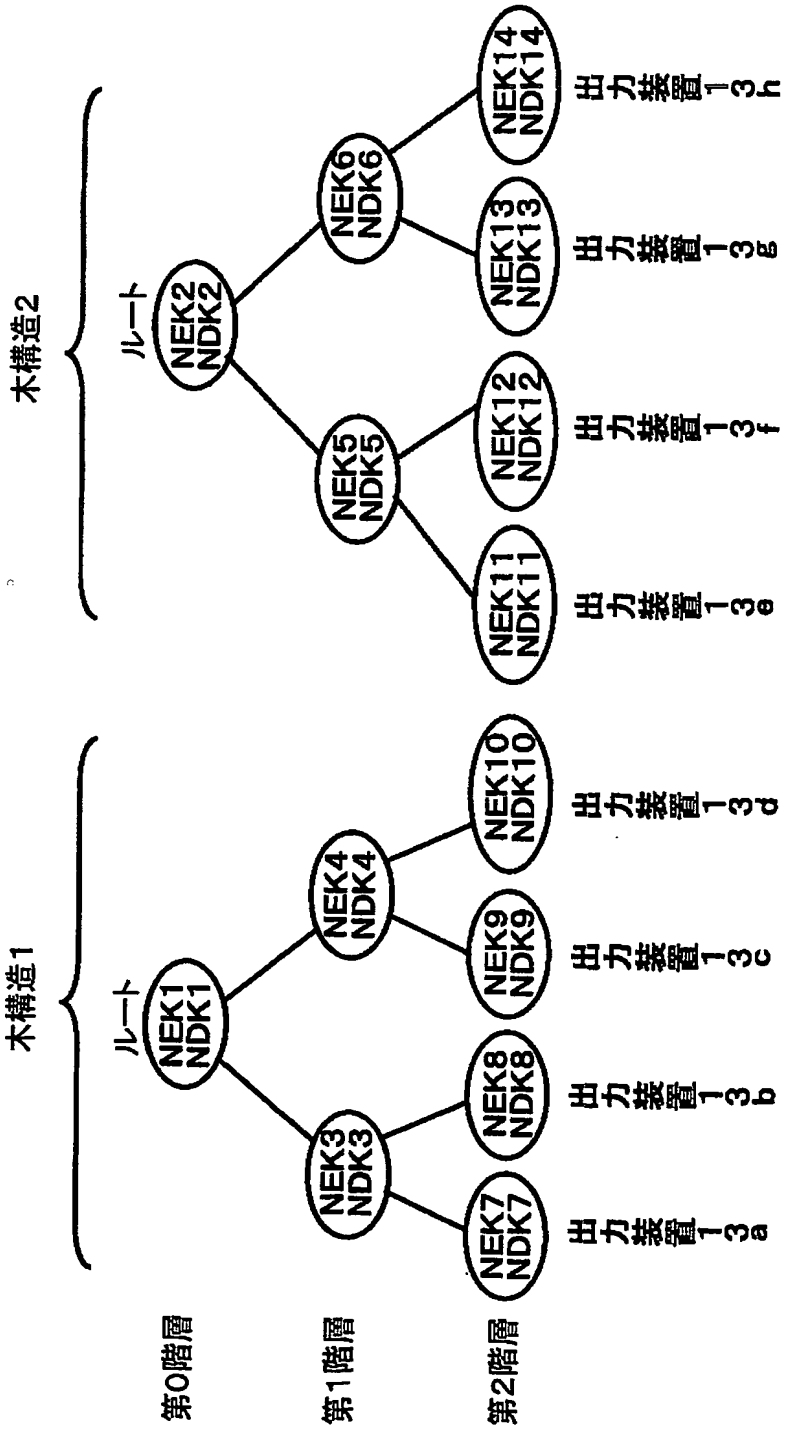

≪暗号化コンテンツ受信時の動作≫
処理開始
コンテンツをサーバから受信したか？
No
Yes
S1301
暗号化コンテンツ鍵群を復号化鍵取得部へ出力
S1302
割当ノード復号化鍵群を取得
S1303
暗号化コンテンツ鍵群から復号化鍵を取得
S1304
コンテンツ復号化鍵を第一復号化部へ出力
S1305
コンテンツ復号化鍵を基に
暗号化コンテンツを復号化
S1306
復号化コンテンツを出力部へ出力
S1307
復号化コンテンツを外部へ出力
S1308
処理終了

【図２２】


≪鍵更新情報受信時の動作≫
処理開始
鍵更新情報を受信したか？
No
Yes
S1351
鍵更新情報を第二復号化部へ出力
S1352
個別鍵格納部から出力装置識別子と個別鍵を取得
S1353
対応する暗号化割当ノード復号化鍵群を取得
S1354
個別鍵に基づき暗号化割当ノード復号化鍵群を復号化
S1355
割当ノード復号化鍵群をノード鍵格納部へ格納
S1356
処理終了

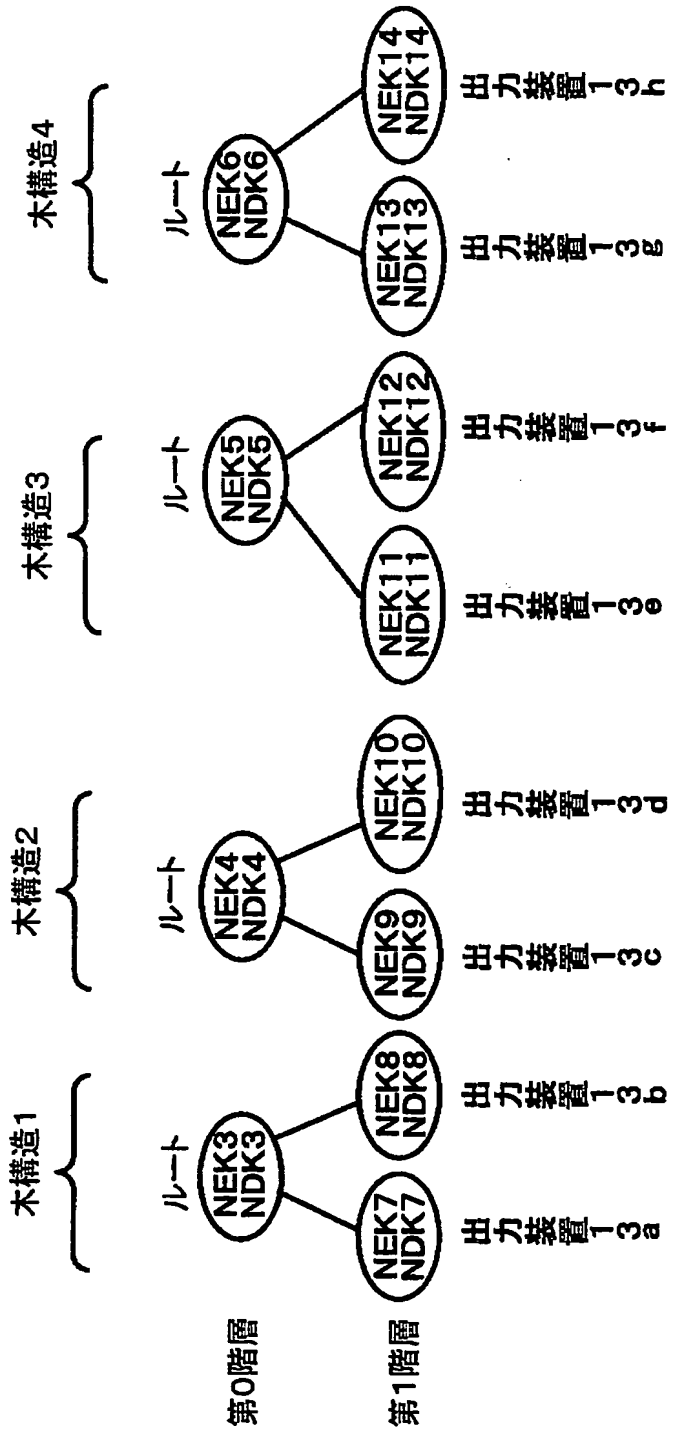
【図２３】

出力装置13a～13hに対するノード暗号化鍵及びノード復号化鍵の設定方法の別の一例



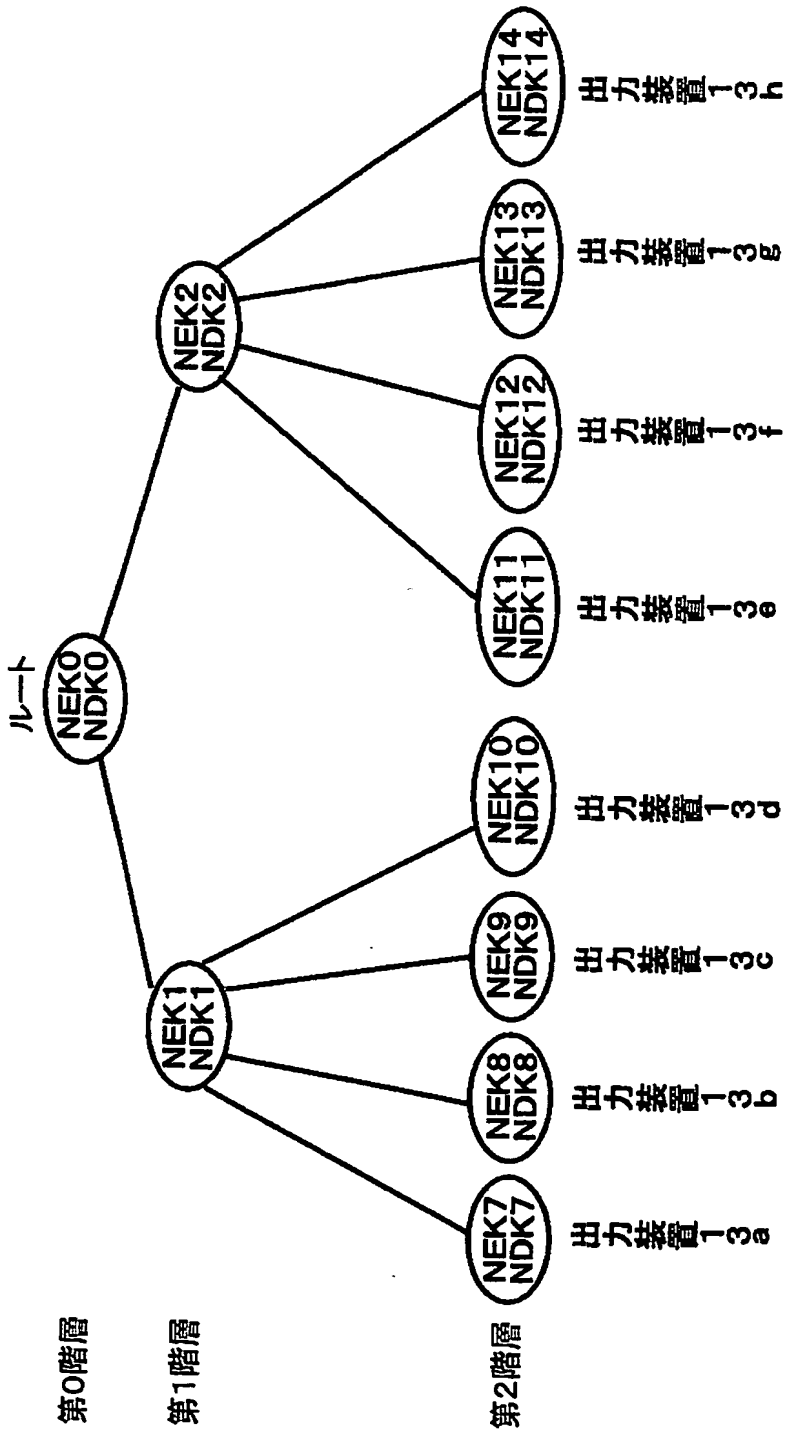
【図２４】

出力装置13a～13hに対するノード暗号化鍵及びノード復号化鍵の設定方法の別の一例



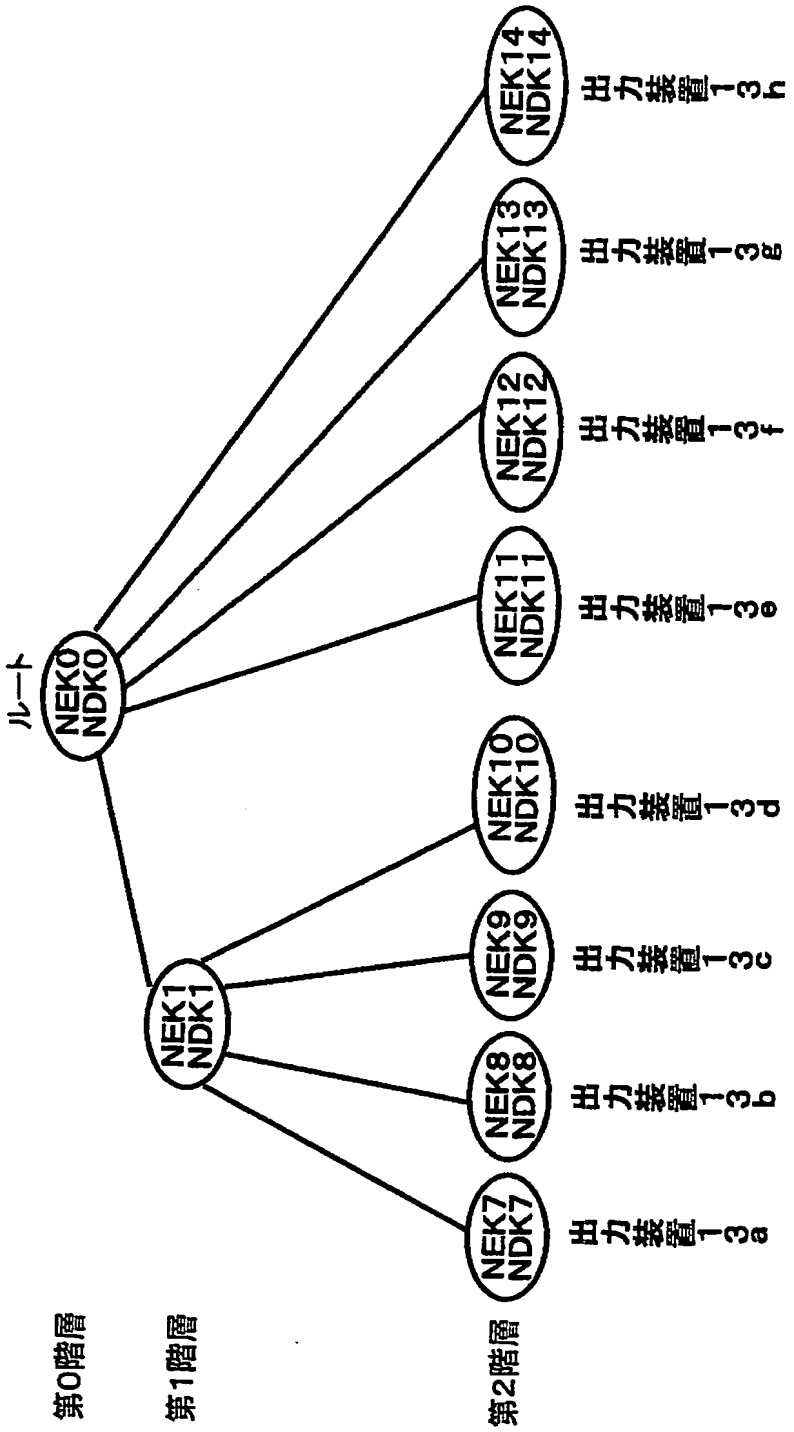
【図２５】

出力装置13a～13hに対するノード暗号化鍵及びノード復号化鍵の設定方法の別の一例



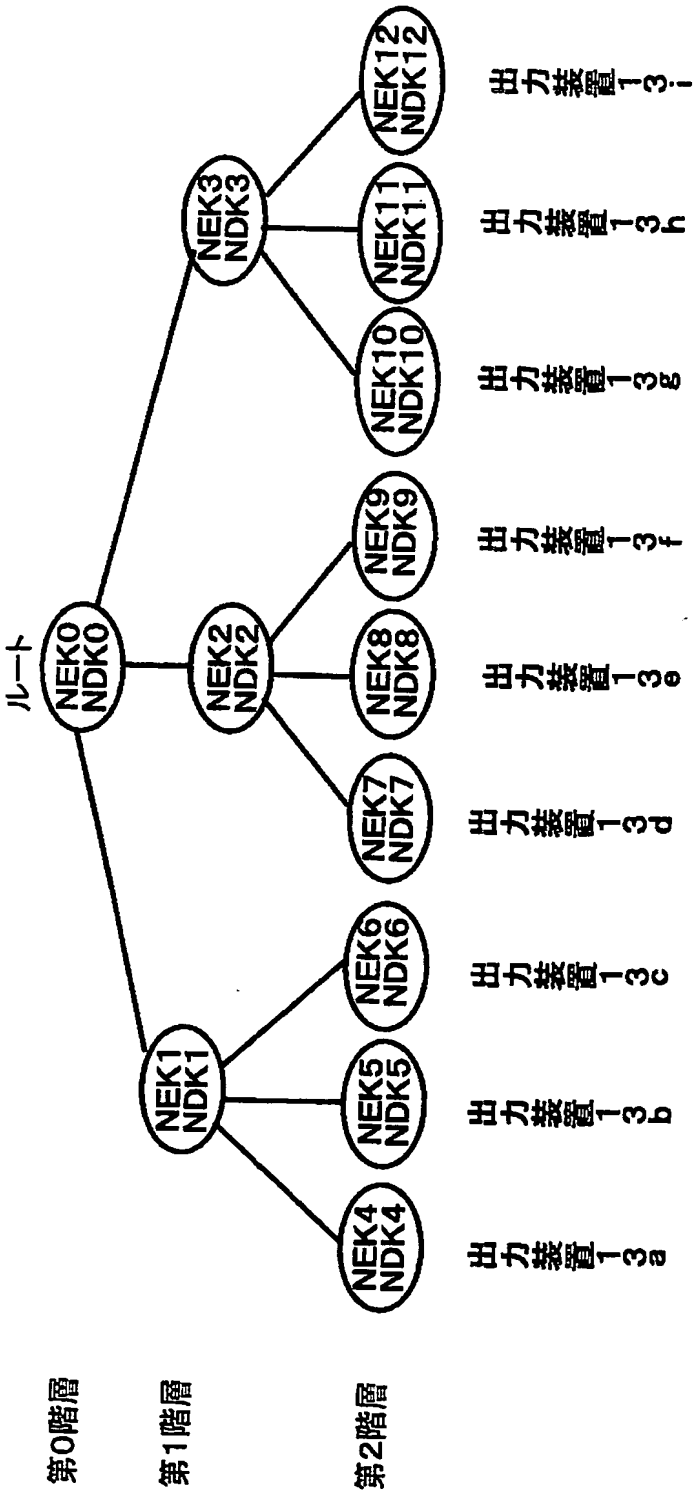
【図２６】

出力装置13a～13hに対するノード暗号化鍵及びノード復号化鍵の設定方法の別の一例



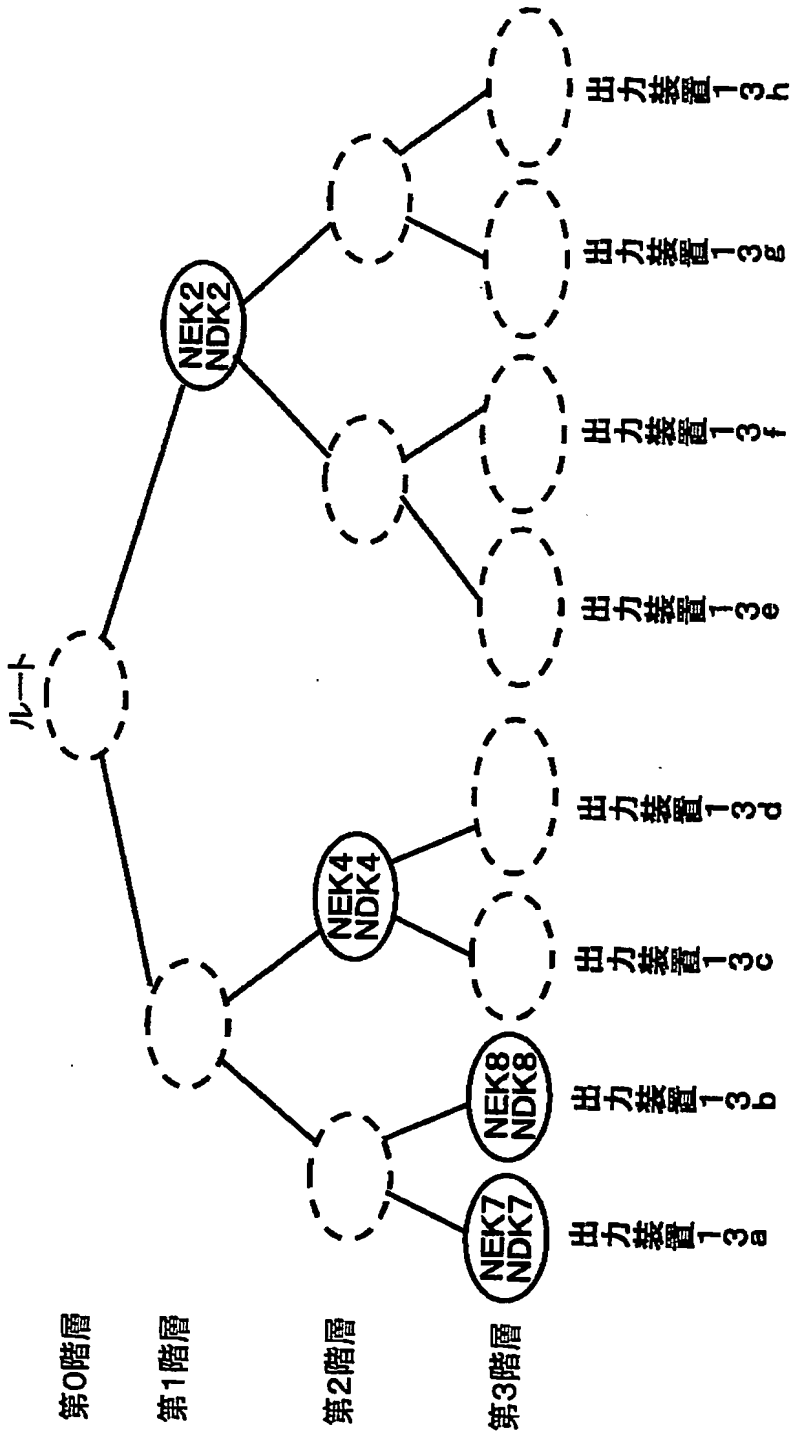
【図２７】

出力装置13a～13hに対するノード暗号化鍵及びノード復号化鍵の設定方法の別の一例



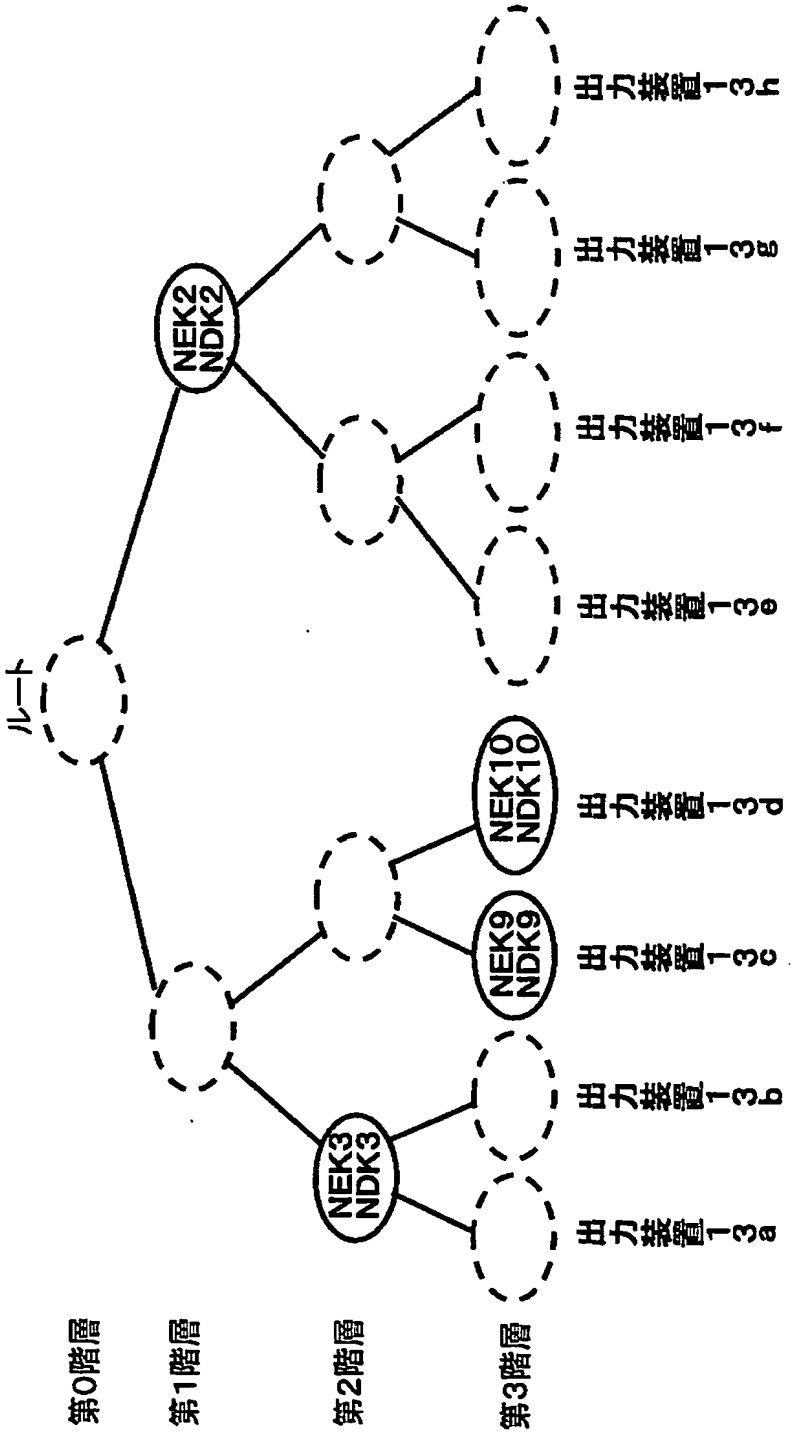
【図２８】

コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例（割当ノード復号化鍵群）



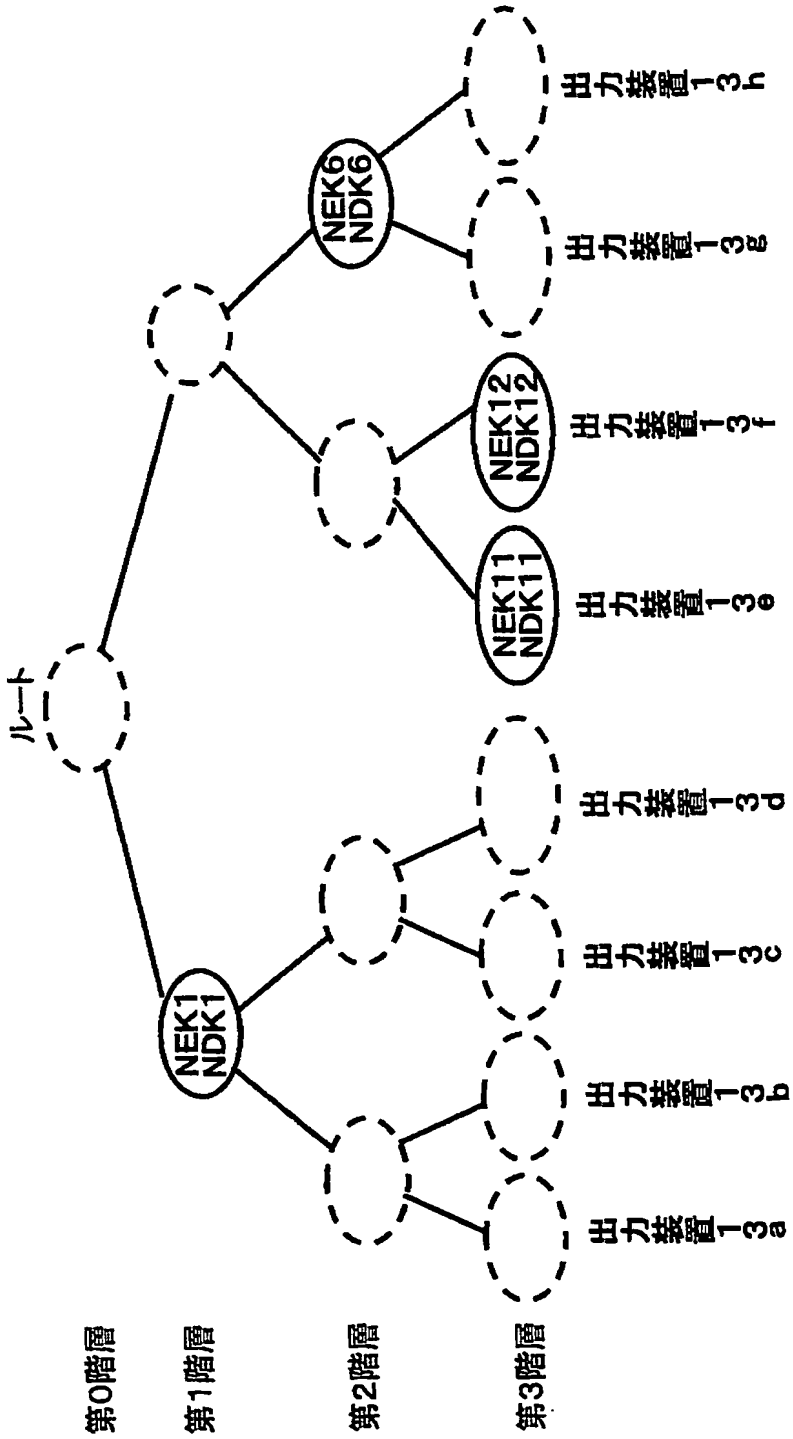
【図２９】

コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例（割当ノード復号化鍵群）



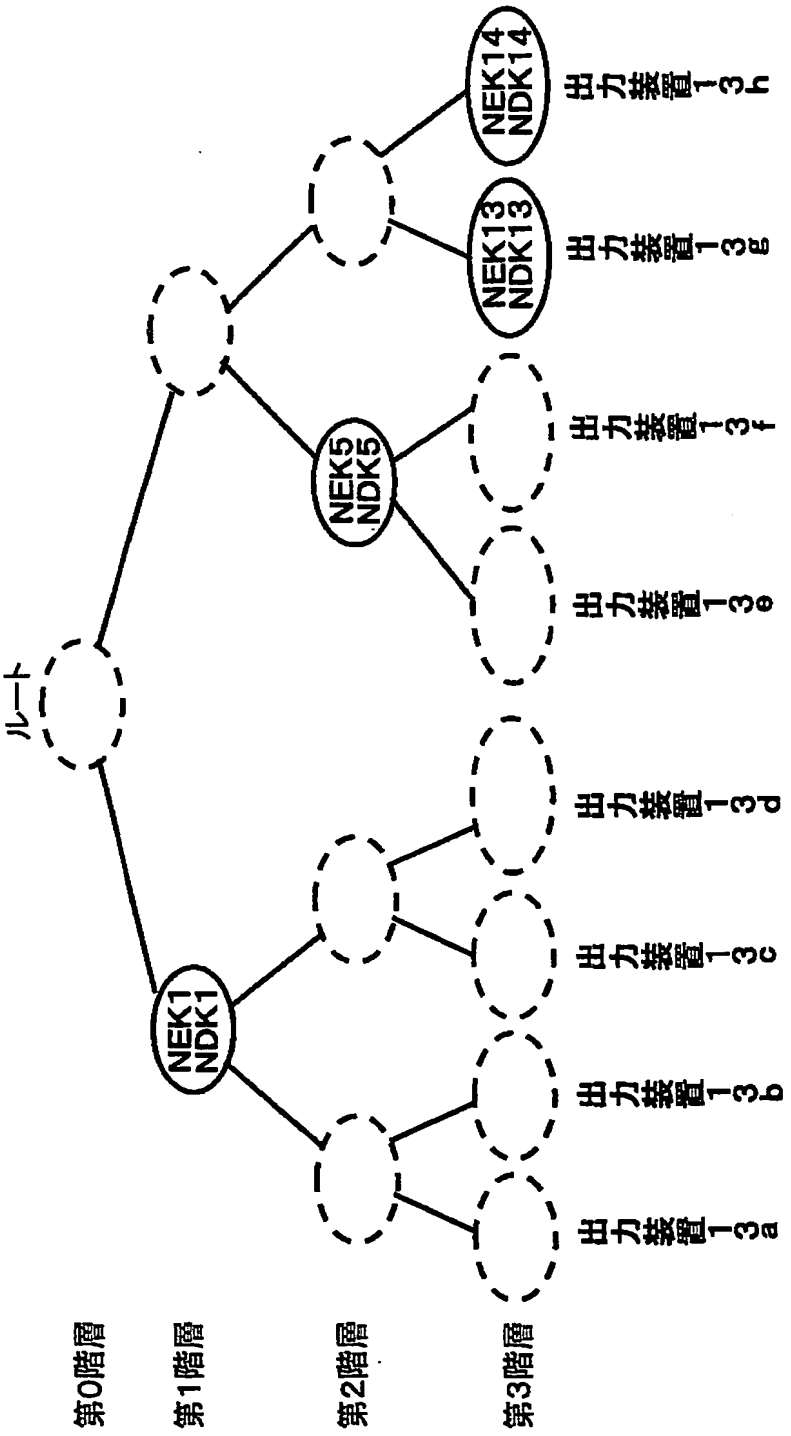
【図３０】

コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例（割当ノード復号化鍵群）



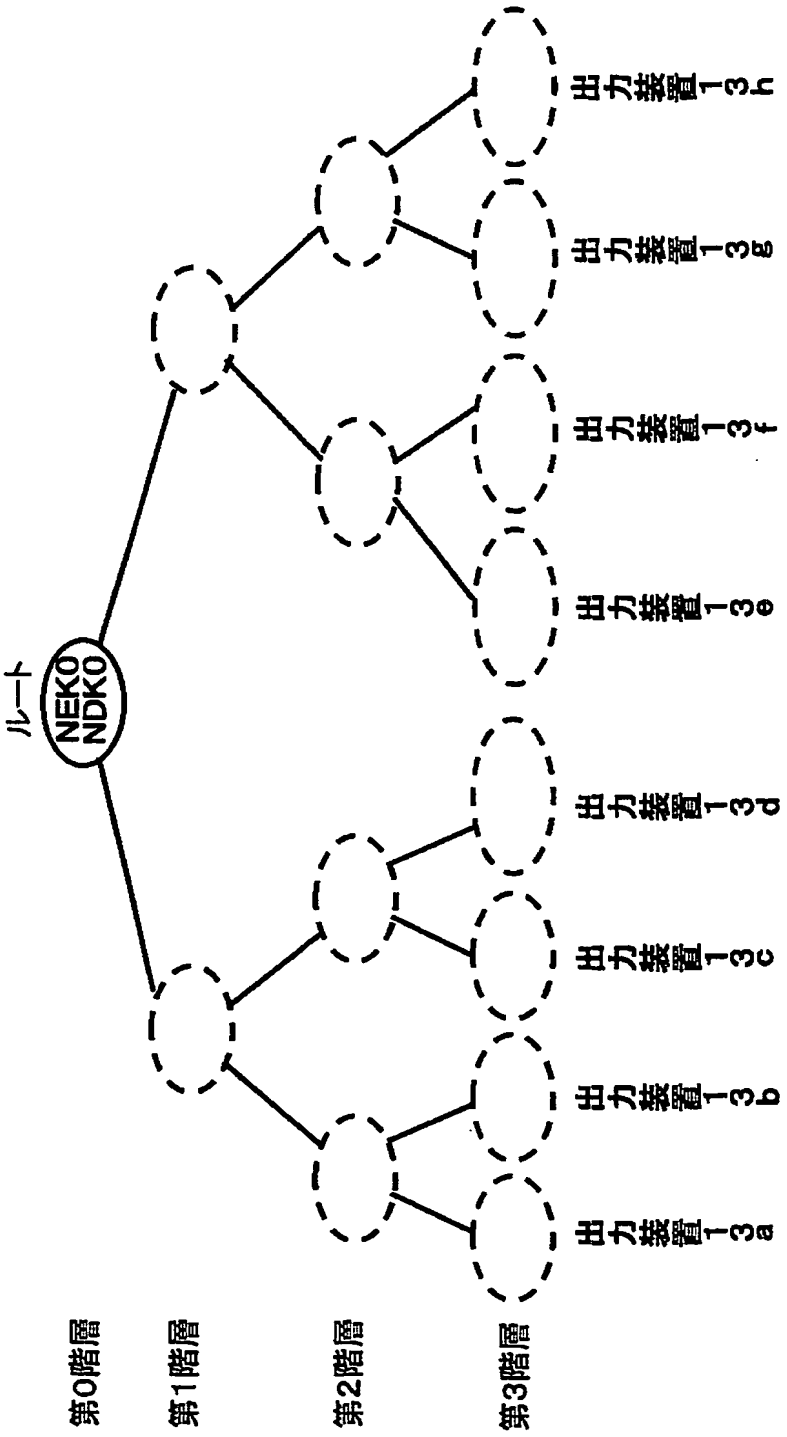
【図３１】

コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例（割当ノード復号化鍵群）



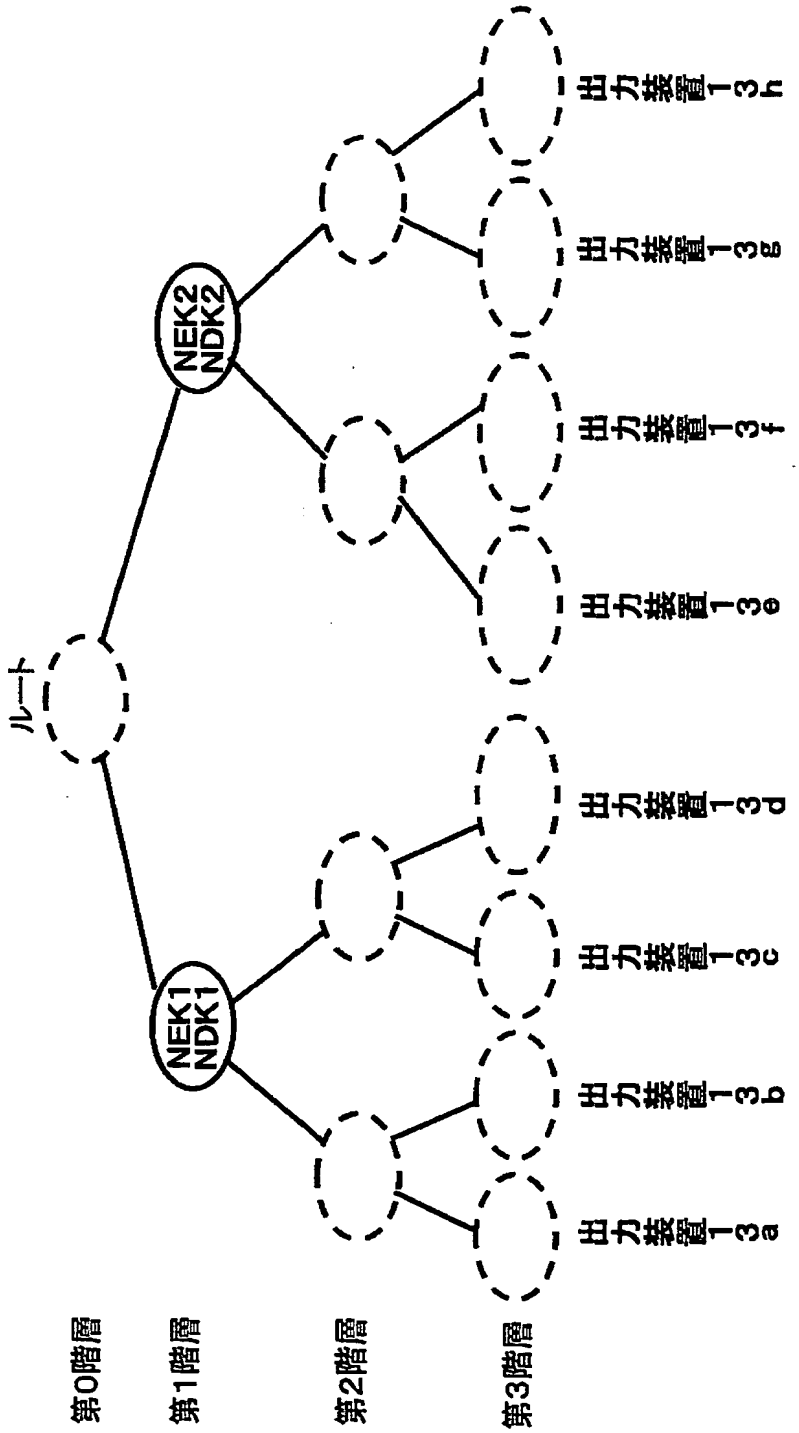
【図３２】

コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例（割当ノード復号化鍵群）

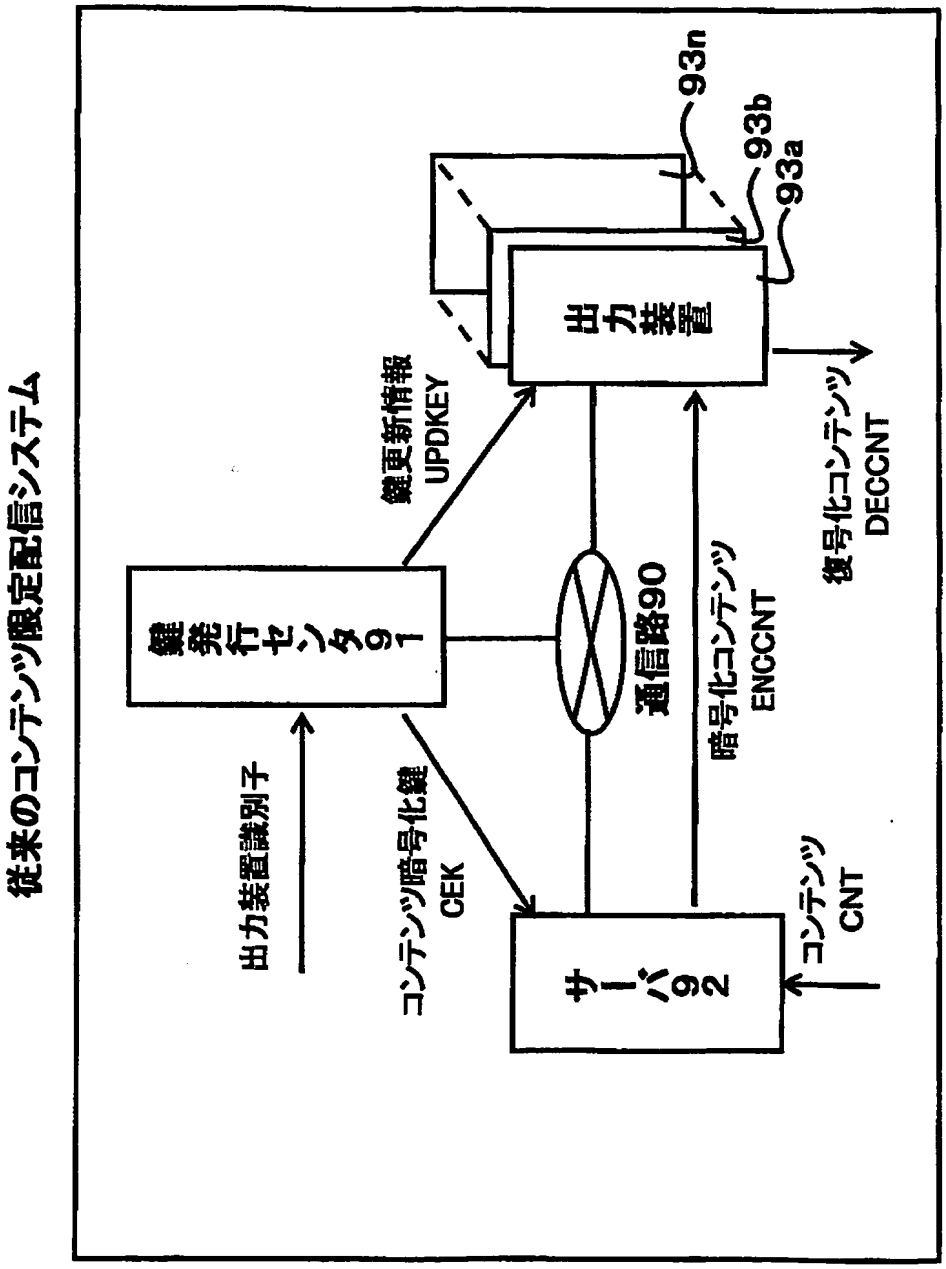


【図３３】

コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例（割当ノード復号化鍵群）



【図３４】


従来のコンテンツ限定配信システム
鍵発行センタ91
サーバ92
出力装置
通信路90
出力装置識別子
コンテンツ暗号化鍵
CEK
鍵更新情報
UPDKEY
暗号化コンテンツ
ENCCNT
復号化コンテンツ
DECCNT
コンテンツ
CNT
93n
93b
93a

【書類名】要約書
【要約】
【課題】　コンテンツ鍵を更新する毎に送信する鍵更新用データサイズが大きかった。
【解決手段】　本発明は、コンテンツを配信するコンテンツ配信システムであって、鍵発行センタ１１と、サーバ１２と、８台の出力装置１３ａ～１３ｈとが接続されている通信路１０とから構成される。ここで、鍵発行センタ１１と出力装置１３ａ～１３ｈの全ての組には、予め各々の組が共有している一つの個別鍵が与えられており、例えば鍵発行センタ１１と出力装置１３ａは個別鍵ＩＫａを、鍵発行センタ１１と出力装置１３ｂは個別鍵ＩＫｂを、鍵発行センタ１１と出力装置１３ｈは個別鍵ＩＫｈを予め共有している。
【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－４１９７６５
受付番号	５０３０２０７８１１８
書類名	特許願
担当官	第三担当上席　　００９２
作成日	平成１５年１２月１８日

＜認定情報・付加情報＞

【提出日】　平成15年12月17日

特願２００３－４１９７６５

出願人履歴情報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/019124

International filing date: 15 December 2004 (15.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2003-419765
Filing date: 17 December 2003 (17.12.2003)

Date of receipt at the International Bureau: 10 February 2005 (10.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse